SSQ
STRATEGIC STUDIES QUARTERLY
WINTER 2015 VOL. 9, NO. 4

Commentary

Strategic Studies Quarterly (*SSQ*) (ISSN 1936-1815) is published quarterly by Air University Press, Maxwell AFB, AL.

Strategic Studies Quarterly

An Air Force-Sponsored Strategic Forum on National and International Security

VOLUME 9 WINTER 2015 NUMBER 4

Commentary

Feature Article

Perspectives

Book Reviews

An Aerospace Nation

Aerospace is deeply connected to US identity—its power and place in the world. Progress in aerospace opened doors to new methods of travel, economic prosperity, and the means to shelter and defend the nation. However, the rapid development of aerospace power was not something left to chance. Such an achievement was a national priority—one that called together all aspects of American society. Military experts worked closely with civilian engineers to refine requirements; academics contributed to designs, while machinists worked with designers. This kind of collaboration formed the United States as an aerospace nation, and aerospace industries remain critical to the US economy, the American people, and the American way of life. Now is the time to consider a short historical view of the impact aerospace has had on the United States and also to warn about the costs of neglect. More importantly, the nation must have a new vision for the future of aerospace.

The Rise of the Aerospace Nation

During the middle of the twentieth century, the US aerospace industry grew tremendously, resulting in the United States emerging from World War II with the world's most advanced commercial infrastructure and preeminent economy and as the world's only nuclear super power.[1] This industry created the foundation upon which the US economy rests and continued to ingest heavy investment for several decades—while providing a major source of American power.[2] In addition to doubling human productivity, becoming an aerospace nation was a critical pillar of economic growth for the United States.[3] Doing so allowed the United States to reap dividends in defending the nation's interests. Capabilities developed by advances in aerospace enabled reduced defense spending as a result of our technological asymmetric advantage. These "offset" reductions in defense spending allowed for development elsewhere in the US economy.

The authors would like to recognize the efforts and ideas of Lt Gen Glenn Spears, retired; Maj Gen Bill Chambers, retired; Maj Gen Waldo Freeman, retired; Col Ronald Banks; Col Douglas Demaio; Col Clint Hinote; Col Tony Meeks; Col Kyle Robinson; Dr. Everett Dolman; Mr. Harry Foster; Mr. Steve Hagel; and Mr. James Mock for their contributions to this article.

The first offset resulted from rapid advancement in the key areas of propulsion, aerodynamics, flight controls, avionics, and human factors that were achieved in the 1950s and beyond. America, as an aerospace nation, served as the essential integrator for these technologies. The aerospace community united for the "first offset strategy" of integrating nuclear warheads on bombs and missiles, which enabled Pres. Dwight Eisenhower's "New Look" strategy—cutting the defense budget by 40 percent between 1952 and 1956. The United States relied on its aerospace superiority to offset Soviet military might without sacrificing the security of our nation or commitments to allies and partners.[4]

The second offset resulted from technological investments in sensing; precision navigation and timing; intelligence, surveillance and reconnaissance; and stealth technologies. Again, US supremacy in the aerospace arena enabled smaller numbers of weapons to be used to hit and destroy key military targets. These investments enabled lower procurement numbers of advanced platforms, saved billions of dollars, and kept the United States ahead of the rest of the world as an aerospace nation.[5]

The payback to the economy and to the taxpayers from these aerospace investments remains significant. Today, this industry—from private aircraft manufacturers, to general aviation, to commercial space—produces $118.5 billion in export sales for the United States, results in approximately $370 billion in domestic aerospace purchases, and employs or supports more than 1.849 million people, whose spending employs 2.51 million more. The aerospace industry is the fifth-largest contributor to the gross domestic product (GDP) of the United States, behind only health care, chemicals, the food industry, and information technology.[6] Of these five, only the food industry also produces a positive export balance for the United States, making the aerospace industry a key component of balancing US foreign trade.[7] It contributes to America's ability to "respond to threats such as terrorism, environmental disasters, and pandemics."[8]

In addition, there are new technologies and businesses that emerge as a result of aerospace investments. Each year, NASA publishes a book called *Spinoff* that highlights its return on investment, often estimated to be several dollars of impact for every dollar spent.[9] Small samples of the job-creating technologies that have emerged from these investments include the following:

- Filtration systems that have brought cheaper and more accessible drinking water to millions throughout the world
- Bioreactors that sparked creation of a new multimillion dollar line of healthy organic juices[10]
- Insulating aerogels that create more durable outerwear from the materials that keep our astronauts insulated from the extremes of space (these same gels are also now being used in building materials improving energy conservation)[11]
- New coatings that increase solar collector efficiency
- Antigravity treadmills developed to train astronauts that are now being used to rehabilitate patients with serious arm and leg injuries.

There are numerous industries that boost our economy and improve our quality of life that emerged from US aerospace investments. Despite these successes, America cannot take this source of technological innovation for granted.

The Cost of Neglect

The story of America's rise to become an airfaring nation is a proud one, but the gains won by hard work are quickly being lost. The status of nation-states can rise and fall quickly. For example, in 1900, Great Britain was the richest nation in the world. Boasting the planet's most powerful military, Britain was the center of world commerce, information, and finance. Its education system was second to none, and its currency was the world's benchmark. In the early part of the twentieth century, the British Empire covered one-fifth of the world's territory and included a quarter of the world's population. Yet four decades after the declaration of the Aerial League of the British Empire, that prominence crumbled and the era in which Britannia ruled the seas gave way to "the American Century."[12]

A similar shift is now under way in the United States. A former chief executive officer (CEO) of American Airlines lamented, "[We are] now laggards in every category."[13] Once we were visionaries, and integrated aerospace was a core cultural, industrial, intellectual, and even aspirational tenet of American power. Now, America has atrophied from its natural curiosity and the frontier of discovery.

Today, the average citizen's experiences with aerospace are no longer inspirational; they are mundane and tired. In 2014 none of the top 25 airlines were American.[14] A far cry from the ambition of Pres. Harry Truman and Gen Jimmy Doolittle, our airports also lag. As of March 2015, the United States had no airports in the world's top 25, and 19 nations had superior airport infrastructure to the top-rated American airport in Cincinnati. Our newest airport, Denver International, the multibillion dollar five-year construction project that concluded with a malfunctioning luggage system, came in second in the United States and 37th place in the world.[15] Meanwhile, nations such as China build new aviation facilities more quickly and to a higher standard than we do. China is planning to spend the equivalent of $250 billion building their aerospace industries of the future and is the site of over two-thirds of the airports now under construction around the world.[16] Beijing International, completed in half the time of Denver,[17] is one of the world's top-10 airports and handles seven times the passengers of Denver International.[18] In some Chinese cities, the airport developers are being advised by a leading American proponent of the airport-centered city, or "aerotropolis."[19]

Thus, it is no surprise so many in America seek their dreams and employment outside the aerospace sector.[20] Tech savvy Millennials gravitate to Silicon Valley not Palmdale, California, or Dayton, Ohio. Aviation innovation in America seems on laissez faire–neglect autopilot, disconnected from national goals and policy that nurtured it and America to greatness. While 600 million people watched Apollo 11 landing on the moon, only 11,000 watched SpaceShipOne win the $10 million Ansari XPRIZE.

Loss of Competitiveness in Aerospace

In the critical area of space, the United States is losing market share. It fell from being the dominant space power with 31 new satellite orders—more than 54 percent of the world's total in 2008—to only 32 percent of global orders in 2013 and only 11 new satellite orders in 2014. This represents a 22-percent loss in world share in only five years.[21] The situation is no better in airplane manufacturing. US competitiveness, which is already eroding compared to European competition, appears about to erode further—damaging a major component of

the US economy. Total employment in the aircraft portion of the aerospace industry has declined almost 20 percent from a peak of 741,100 in 1998 to only 606,000 today.[22] Airbus consistently challenges Boeing as the world's principal airline platform, while China—able to undercut both American and European wage structures—has just entered the market.[23] Without bold leadership and deliberate revitalization, US market share is likely to decline further. The new Chinese manufacturer, Commercial Aircraft Corporation of China (Comac), has already won 400 orders for its C919 airliner, an aircraft in the same large commercial class as the Airbus A320 and Boeing 737. This number is roughly equivalent to an entire year's large aircraft order share of Boeing or Airbus in recent years.[24]

America's leadership in the high-technology sector is also faltering and, if not corrected, will put downward pressure on our economy. Of the 50 advanced industries, aerospace is one of only nine that are contributing to reduced trade deficits. It is also the largest of these industries in its contribution to the US balance of trade. Yet, in high-tech jobs, America is declining. The share of advanced technology jobs in the United States lags behind the Czech Republic, Slovenia, Germany, Hungary, Sweden, Finland, Italy, Denmark, and Austria. Further, with one of the steepest rates of decline in these sectors in the developed world, the United States is poised to fall behind France, the Netherlands, Norway, and Belgium over the next several years.[25]

A lack of people educated in science, technology, engineering, and math (STEM) in the workforce is part of the US problem. In 2013 a Price Waterhouse Cooper survey of CEOs found that 54 percent of aerospace companies view the lack of available skills as the most significant threat to company growth. Other nations are graduating more engineers and hard-science professionals than the United States. An estimate by the US Department of Commerce predicts that by 2018 "the U.S. will have more than 1.2 million unfilled STEM jobs because there will not be enough qualified workers to fill them."[26] Reviving the aerospace nation begins with recapturing the magic and mystique of the first decades of aerospace innovation for our youth. If the United States fails to motivate the new generation to become part of something more and if it fails to attract the technicians and engineers to make a difference in its high technology industries, the US decline relative to other

states will continue, causing the American Century to give way to the Asian Millennium.[27]

Being an aerospace nation has paid vast dividends to the US economy in the past, and it can again. Beyond creating more than 4 million jobs tied to aerospace, investments in these industries help create a better life for Americans. In 2014 NASA estimated technology it originally paid for and developed saved 449,850 lives (equivalent to the entire population of Atlanta), created nearly 19,000 jobs (the approximate seating capacity of Madison Square Garden), generated $5.2 billion in revenue for commercial companies (or more revenue than for all concerts held in North America), and reduced the costs of living for Americans by $18.6 billion (more than the total revenue for the global airline industry).[28]

Investments in these enterprises reap great rewards, and American investment in aerospace has never failed to pay off. The aerospace investments made in 2010 returned $37.8 billion in tax revenue to the US treasury in that year alone.[29] Most of these investments will continue to pay additional dividends in the years that follow or generate spinoff companies that will pay future dividends to the taxpayer as these nascent businesses and industries grow. While precise estimates vary based on specific study methodology and the timeframe analyzed, the dollars invested by the government in the aerospace industry have created large numbers of private-sector jobs and spinoffs, with a return to the treasury that is well over one dollar of tax revenue for each dollar spent, making the aerospace industry one of the few places where increased government spending actually makes money for the taxpayer.[30] Thus, being an advanced aerospace nation will help balance the federal budget and extend the benefits of prosperity to a new generation. What the United States needs now is a vision of where aerospace could take it and a strategy to get there.

A Vision for the Future

The United States can reinvigorate its aerospace industry into a globally admired enterprise that again becomes the engine for innovation, business development, and commerce for the nation. However, this will require the combined efforts of all its citizens: engineers, industry, academia, and the military. While we have a model on which this was

done under the stress of nuclear and space competition in the 1950s, a broader model is needed now.[31]

In 1946, to help the aerospace industry grow, President Truman issued Executive Order 9781, establishing the Air Coordinating Committee, with the mission to "examine aviation problems and development affecting more than one participating agency; develop and recommend integrated policies to be carried out and actions to be taken."[32] Through interdepartmental cooperation between the Departments of State, War, Navy, Commerce; the Post Office; and the Civil Aeronautics Board, the United States created the airspace structure that became the model for the world and created a vision for space activities that would enable that nation to compete in the space race. Today, with a broader range of challenges before us, a similar but broader construct is needed.

Therefore, the United States must establish a National Aerospace Coordination Council. This council would be responsible for providing the interagency coordination required to implement the National Aerospace Strategy. Responsible directly to the president, the council should—at a minimum—be comprised of representatives from NASA, the Federal Aviation Administration, the White House Office of Science and Technology, and the Departments of Education, Commerce, Energy, Homeland Security, and Defense to coordinate and implement the steps governing the reinvigoration of our STEM education and aerospace infrastructure enterprises. This council should also be infused with—or regularly consult—the captains of the aerospace industry. Its central role will be to enable a path forward whereupon innovation, commerce, logistics, and new scientific breakthroughs can be accelerated using all forms of aerospace technology, including robotics, drones, information technologies, energy research, and aerospace design.

Establish a New Air and Space Structure

Like its predecessor, this council will, as one of its deliverables, define an airspace utilization plan for the twenty-first century. This plan needs to accommodate large fleets of unmanned vehicles that may deliver goods and services transiting the national airspace, potentially in close proximity to aerodromes, while operating autonomously and outside the line of sight of any human director. This construct needs to accommodate logistics paradigms, such as drone delivery of goods and services to one's doorstep—as well as transit from the existing airspace structure

to and from space.[33] Once developed, this system should be promulgated to the International Civil Aviation Organization for international implementation.

Double Down on Far-Term Investments

This council will be empowered to coordinate research efforts into aerospace technologies to coordinate the movement of aerospace advancement across the spectrum. Investments by the Department of Education and Department of Defense laboratory system, the Defense Advanced Research Projects Agency, and the National Oceanic and Atmospheric Administration can be leveraged cooperatively to move forward new aerospace structural concepts, including the blended-wing body and new engine designs like the Air Force's Adaptive Versatile Engine Technology (ADVENT) program or NASA's Environmentally Responsible Aviation project. With industrial representation, these breakthroughs can be shared with the captains of US industry, enabling these leaders to market breakthrough technologies that will enhance their market share of emerging and new business opportunities. Within this investment portfolio, the council will ensure basic science and technology research with an eye toward the future. At present, these investments represent a very small fraction of the research enterprise; thus, increasing these investments carries little cost. Nonetheless, seed money for technologies such as extraction of minerals from celestial bodies, diversion of asteroids from Earth orbit or collision, and efficient power collection and storage in space are among the spacefaring capabilities that should serve as a guide for longer-term investment.

Begin a New Series of Innovation Prizes

New technologies will be required across the aerospace spectrum, ranging from the control of unattended drone delivery of goods and services to establishing new capabilities in space. To this end, the government—alongside the private sector—should incentivize the collective engineering intelligence of the nation by creating a series of "X-Prizes" for breakthroughs in key technologies. Among those that may need emphasis are precise navigation and timing and applied autonomy technologies. The council will work to ensure these competitions are aimed at and designed to develop and implement the national aerospace utili-

zation promise outlined above and to enable the exploration of space as described below.

Increase Tolerance for Risk and Adventure

The United States needs a renewed commitment to innovation and to risk. Research involving science and technological risk is critical to advancing the aerospace industry and creating new spinoff technologies and businesses that create jobs for America. Research involving little or no risk pays little or no dividends, and if we are not occasionally failing in attempts to push the science-and-technology envelope, that means we are not trying.[34]

As Pres. John F. Kennedy said in 1962, "We choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills."[35] As President Kennedy articulated, the nation needs lofty goals. Therefore, the council will, as it directs the research and development spending, deliberately vector some of this funding to projects that may fail—and may even do so spectacularly. However, such failures teach us how to get the hard science right the next time. Thus, failing early, often, and sometimes even loudly needs to be an accepted cost of engaging in leading-edge research.[36]

Create a New National Aerospace Infrastructure Plan

The council will explore national aerospace infrastructure needs, including airspace, routing, and terminal facilities for both air and space travel. Development of innovative facility design to ensure proper passenger and commercial shipment security while providing world-class experiences for passengers will be a major priority. To instill a sense of wonder in aerospace, flying by the general public must again be a wondrous experience. The council should give consideration to leasing or sharing arrangements with existing government aerospace infrastructure, including the space-launch facilities in Florida and California. Arrangements that enable commercial exploration and experimentation in and through the aerospace domain should be a priority. Integration of privately developed air and space ports into the national aerospace infrastructure should also be undertaken.

Prioritize National Science Activity

The council will be charged with enhancing STEM education across the United States. Partnering with our best engineering institutions and with industry, the council will coordinate joint private/public-funded scholarship opportunities to create an incentivized pathway for 1.5 million secondary students to obtain STEM degrees.[37] Those who take these scholarships would study in defined degree areas and then pay back their scholarship by working either for the government agencies and/or the private companies that funded their education, thereby addressing the STEM shortage.[38] This coordination would allow for targeted recruiting by government and industry of desired skill sets, diversity, and the technological breadth that would optimally move the aerospace sector forward.[39] This initiative would more than pay for itself. The advanced industries that have grown out of our STEM investments to date will add $2.7 trillion to the US GDP—or about 17 percent of the total this year.[40]

Prioritize Space Development and Set Ambitious Goals

The council will take for action the consensus recommendation of NASA's 2015 Pioneering Space National Summit. The joint statement of the approximate 100 attendees was that "the long term goal of the human spaceflight and exploration program of the United States is to expand permanent human presence beyond low-Earth orbit in a way that will enable human settlement and a thriving space economy. This will be best achieved through public-private partnerships and international collaboration."[41] While not fully implementable in the next 20 years, the council will lead a public-private partnership to begin to solve the key challenges in space. America needs to be the first nation to establish a propellant depot in space, the first to conduct space refueling, the first to mine the moon or harvest asteroids, and the first to construct a permanent settlement in space.

Invest in Promising Technologies

Lastly, the council will leverage the best scientific and strategic minds across the government enterprise to explore whether a new synergistic use of emerging technologies may enable new strategies to defend the homeland across the interwoven dimensions of land, sea, air, space, and

cyberspace, while projecting power around the globe. Investments in power, propulsion, and sensors have historically paid dividends. New technology vectors such as autonomy, swarming, directed energy, independent precision navigation, and timing are all showing rapid advances toward potential breakthroughs. Specifically, the council will pursue a portfolio development approach to explore whether the ability to network myriad small systems with larger systems into a seamless but massed force could enable the military to conduct operations in ways never before envisioned. A true third offset will be more than about airplanes or new computers. It will depend on people and require the United States to maintain its aerospace technology leadership over all competitors—a lead we are not guaranteed to maintain. It requires the United States to again bring engineers, academics, business leaders, and government together as an aerospace nation.

Conclusion

The widespread benefits of aviation did not just happen. They were the result of deliberate strategy by both civilian and military thinkers who understood the far-reaching value of aviation in a time when American leadership was shaping the institutions of the world and the industrial policy at home. Over the next 20 years the United States will open the door to the markets of the 3 billion people in the developing world. It will develop a method of coordination of lower airspace infrastructure in a manner that enables safe and efficient transportation of materials by drone or other robotic devices from any place to anywhere. The country will reinvent its domestic aerospace infrastructure such that it leads, not lags, the world. It will create new engine designs based on programs such as the ADVENT and Environmentally Responsible Aviation research efforts that will improve fuel efficiency—potentially making the United States the engine supplier of choice for the world—while reducing costs of travel for passengers and logistics alike.[42] It will create new blended-wing body aircraft that will be more aerodynamic and more efficient, enabling airlines and logistics to be conducted more efficiently with designs that no other country can match.[43] The nation will invigorate light-aircraft manufacturing to become the chief suppliers of small aircraft for emerging air service routes in areas such as the awakening countries of Asia and Africa.[44] It will set sights on rekindling

spacefaring interests to expand not only exploration but also exploitation of resources that exist in space. The country will enable commercial interests to begin ventures that explore and profit from the vast mineral and power resources that lie on the moon and within earth orbit, while developing systems that can mitigate the risk from asteroid strikes.[45] The United States will do all these things while ensuring the fiscal security of the nation and maintaining our commitments to the American people and allies.

The world is again at a place where US leadership can make a difference. It is again at a place where aerospace vehicles can change the world for the better and where the nation's grand strategy is an aerospace strategy. The recipe for success has not changed: first, have a vision for shaping the aerospace domain, and second, invest in preeminence in aerospace transportation. The future of the United States as an aerospace nation hangs in the balance. We are best as an aerospace nation when our brightest minds, our most innovative industries, and our most critical governmental agencies work together. The future economic prosperity and national security depend on the choices we make now. The steps outlined above form the initial vector to put America back on a trajectory that will lead us higher and farther and extend the blessings of liberty and prosperity to ourselves and our progeny. SSQ

John P. Geis II, PhD
Director of Research, Air Force Research Institute

Lt Col Peter A. Garretson, USAF
Professor, Air Command and Staff College

Notes

1. The US economy grew by 50 percent in the 1940s alone, from $200 billion in 1940 to roughly $300 billion in 1950. However, US dominance as the world's only nuclear power was short-lived. Christopher Conte and Albert R. Karr, *An Outline of the U.S. Economy* (Washington, DC: US Department of State, 2001), http://usa.usembassy.de/etexts/oecon/chap3.htm.

2. Alexander J. Field, *The Great Leap Forward: 1930s Depression and U.S. Economic Growth* (New Haven, CT: Yale University Press, 2011), 1–9. Field argues that the transformational period of transportation, to include land and air, resulted in the highest period of total factor productivity growth in American history from 1928 to 1950. He credits the transportation network, to include aviation, with this dynamic—in what he calls "The Most Technologically Productive Decade of the Century." In the interest of precision, Field argues that the demilitarization of the United States and the failure to invest in aviation technology during

the 1930s was counterproductive in terms of economic growth until 1941, by which time military research and development were again a significant aspect of economic development and human productivity growth.

3. The US economy grew by 50 percent in the 1940s alone, from $200 billion in 1940 to roughly $300 billion in 1950. However, US dominance as the world's only nuclear power was short-lived. Christopher Conte and Albert R. Karr, *An Outline of the U.S. Economy* (Washington, DC: US Department of State, 2001), chapter 3.

4. Zachary Keck, "A Tale of Two Offset Strategies: The Pentagon's New Offset Strategy Is Modeled on Two Very Different Historical Examples," *The Diplomat* (Japan), 18 November 2004, http://thediplomat.com/2014/11/a-tale-of-two-offset-strategies/.

5. Ibid.

6. US Department of Commerce, "The Aerospace Industry in the United States," *SelectUSA* (web site), no date, http://selectusa.commerce.gov/industry-snapshots/aerospace-industry-united-states. The recent Deloitte study on employment in the aerospace industry augment the numbers in this study for employment. See also Deloitte (firm), *The Aerospace and Defense Industry in the U.S.: A Financial and Economic Impact Study* (New York: Deloitte, March 2012), 1–3, 16–19, 22, https://www.aia-aerospace.org/assets/deloitte_study_2012.pdf.

7. The Foreign Trade Division of the Census Bureau reports trade statistics through its publications and USA trade online portal. This represents Deloitte analysis of these statistics. Ibid., 21, 78.

8. Mark Muro, Jonathan Rothwell, Scott Andes, Kenan Fikri, and Siddharth Kulkarni, *America's Advanced Industries: What They Are, Where They Are, and Why They Matter* (Washington, DC: Brookings Institute, February 2015), 14, http://www.brookings.edu/~/media/Research/Files/Reports/2015/02/03-advanced-industries/final/AdvancedIndustry_FinalFeb2lores.pdf?la=en.

9. Several studies have looked at the return on investment to the economy of aerospace nation developments. In 1971, Roberts and his peers found the return on investment from NASA research in the 1960s and 1970 to be $7.24 for every dollar spent. See Robert E. Roberts, Howard M. Gadberry, Robert E. Fleisher, Lawrence L. Rosine, E. Duane Dieckman, and Linda L. Crosswhite, *Economic Impact of Stimulated Technological Activity* (Kansas City, MO: Midwest Research Institute, November 1971), http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19730012250.pdf. These numbers do not count computing advances or the information technology sector, some of which resulted from spinoffs of previous NASA, ARPA, and military investments. More recently, numbers of around 5:1 continue to be found. See Henry R. Hertzfeld, "Measuring the Economic Returns from Successful NASA Life Science Technology Transfers," *Journal of Technology Transfer* 27, no. 4 (December 2002): 311–20. For an up-to-date list of recent NASA technology impacts on business, see National Air and Space Administration, *Spinoff*, 2015, 11, https://spinoff.nasa.gov/flyers.html.

10. John Jones, "Water Treatment Technologies Inspire Healthy Beverages," *Spinoff*, 2012, http://spinoff.nasa.gov/Spinoff2012/hm_1.html.

11. Randall Garber, James Hanna, and Arash Ateshkadi, *California Aerospace Industry Economic Impact Study Final Report* (El Segundo, CA: ATKearney, March 2014), https://www.atkearney.com/documents/10192/4393887/California+Aerospace+Industry+-+An+Economic+Impact+Study.pdf/24234fc6-e19d-4367-8eec-743a92544d33; and "Footwear & Apparel: From Outer Space to Your Inner Space," *Aspen Aerogels* (web site), 2015, http://host.web-print-design.com/aerogel/footwear.htm.

12. Many historians cite the Suez Crisis as the point at which the empire crumbled. See Corelli Burnett, *The Collapse of the British Empire* (London: Morrow, 1972). Henry Luce

was the first to use the term *American Century*. See his article, "The American Century," *Life Magazine* 10, no. 7 (17 February 1941): 61–65.

13. Robert Crandall, former CEO of American Airlines, "Charge More, Merge Less, Fly Better," *New York Times*, 21 April 2008, http://www.nytimes.com/2008/04/21/opinion/21crandall.html.

14. The Skytrax World Airline Awards are the result of surveys from 19 million travelers from around the world. The airline industry recognizes this annual award as a "benchmark of Airline Passenger Satisfaction levels." See "Top 100 Airlines," *World Airline Awards* (web site), 2015, http://www.worldairlineawards.com/Awards/world_airline_rating.html. The top-rated US airlines were Virgin Atlantic, which came in 47th place in the world; Delta, which was 50th; and United, which was 53rd.

15. "The World's Top 100 Airports in 2015," *World Airport Awards* (web site), 2015, http://www.worldairportawards.com/Awards/world_airport_rating.html.

16. James Fallows, *China Airborne: The Test of China's Future* (New York: Pantheon, 2012). See also Fallows's interview on the "Diane Rehm Show." James Fallows, interview by Diane Rehm, *Diane Rehm Show*, 10 May 2012, http://thedianerehmshow.org/audio/#/shows/2012-05-10/james-fallows-china-airborne/106432/@00:00.

17. "(PEK) Beijing Capital International Airport Overview," *FlightStats* (web site), 2015, http://www.flightstats.com/go/Airport/airportDetails.do?airportCode=PEK.

18. David Barboza, "Airports in China Hew to an Unswerving Flight Path," *New York Times*, 3 April 2013, http://www.nytimes.com/2013/04/04/business/global/shanghais-new-air-terminal-sets-the-pace-for-speed-and-ambition.html.

19. "Aerotropolitan Ambitions," *Economist*, 14 March 2015, http://www.economist.com/news/china/21646245-chinas-frenzied-building-airports-includes-work-city-sized-projects-aerotropolitan-ambitions.

20. Scott Thompson, Chuck Marx, James B. Grow, Robert W. McCutcheon, et al., *Aviation's Second Golden Age: Can the US Aircraft Industry Maintain Leadership?* (London: PricewaterhouseCoopers, December 2013), http://www.pwc.com/en_US/us/industrial-products/publications/assets/pwc-commercial-aircraft-industry-future-report.pdf.

21. Data source is the Satellite Industry Association Statistics for October 2013, 2010, and 2008, http://www.sia.org;; and Garber, Hanna, and Ateshkadi, *California Aerospace Industry Economic Impact Study Final Report.* See also Tauri Group, *State of the Satellite Industry Report* (Washington, DC: Satellite Industry Association, September 2014), 24, http://www.sia.org/wp-content/uploads/2014/09/SSIR-September-2014-Update.pdf. Reader should note that part of the decline in the number of satellite orders for 2014 is due to uncertainty in Russian launch capacity caused by the conflict in Ukraine. See Tauri Group, *State of the Satellite Industry Report* (Washington, DC: Satellite Industry Association, May 2015), 25, http://www.sia.org/wp-content/uploads/2015/06/Mktg15-SSIR-2015-FINAL-Compressed.pdf.

22. "Total Employment," Aerospace Industrial Association (web site), 2015, http://www.aia-aerospace.org/assets/Stat_Series_12_Employment_-_2014.pdf.

23. Thomson Reuters (firm), "Airbus and Boeing—Graphic of the Day," *The Knowledge Effect* (blog), 9 January 2012, http://blog.thomsonreuters.com/index.php/airbus-and-boeing-graphic-of-the-day/.

24. Ansuya Harjani, "You May Fly on a Made-in-China Aircraft Sooner Than You Think," *CNBC News*, 12 February 2014, http://www.cnbc.com/2014/02/12/you-may-fly-on-a-made-in-china-aircraft-sooner-than-you-think.html.

25. Muro, Rothwell, Andes, Fikri, and Kulkarni, *America's Advanced Industries*, 6–9.

26. "About PLTW," *Project Lead The Way* (web site), 2014, https://www.pltw.org/about-us.

27. This term was coined in the *Air Force 2025 Study*. See Joseph A. Engelbrecht Jr., Robert L. Bivins, Patrick M. Condray, Merrily D. Fecteau, John P. Geis II, and Kevin C. Smith, "Alternate Futures for 2025: Security Planning to Avoid Surprise" (research paper, Maxwell AFB, AL: Air University Press, April 1996), 79–89, http://www.au.af.mil/au/awc/csat/2025/a_f.pdf. Discussions in the study relevant to the economic competitions are found on 29–30, 34, 45–47, 49–52, 59–61, and 163–97.

28. NASA, "Spinoff" (PowerPoint presentation, NASA, 2015), slide 53, http://spinoff.nasa.gov/Spinoff2015/PowerPoint/Spinoff2015.pptx.

29. Deloitte (firm), *The Aerospace and Defense Industry in the U.S.*, 19.

30. Several studies on NASA and aerospace industry return on investment have been accomplished over the years. Estimates of return on investment are very sensitive to the statistical assumptions made in the analysis. For concerns on the sensitivity of the assumptions to the precise ratio, see Henry R. Herzfeld, *Measuring the Returns to NASA Life Science Research and Development* (Washington, DC: Space Policy Institute, George Washington University, 30 September 1998), and Ken Chamberlain, "Measuring the NASA Stimulus," *National Journal*, 27 August 2010, http://www.nationaljournal.com/njonline/no_20100827_1798.php. The general range of these estimates is between 7:1 and 14:1. See Lauren Lyons, "5 Popular Misconceptions about NASA," *Huffington Post*, 9 September 2013, http://www.huffingtonpost.com/lauren-lyons/misconceptions-nasa_b_3561205.html.

31. Delbert R. Terrell, *The Air Force Role in Developing Outer Space Law* (Maxwell AFB, AL: Air University Press, May 1999), http://www.au.af.mil/au/awc/awcgate/space/terrill.pdf.

32. Harry S. Truman, "Executive Order 9781 – Establishing the Air Coordinating Committee, September 19, 1946," *American Presidency Project* (web site), no date, http://www.presidency.ucsb.edu/ws/?pid=77956.

33. For one such logistics construct, see the "Amazon Prime Air," *Amazon.com*, 2015, http://www.amazon.com/b?node=8037720011.

34. Vanessa Chan, Marc de Jong, and Vidyadhar Ranade, "Finding the Sweet Spot for Allocating Innovation Resources," *McKinsey Quarterly*, May 2014, http://www.mckinsey.com/insights/innovation/finding_the_sweet_spot_for_allocating_innovation_resources.

35. John F. Kennedy, "Text of President John Kennedy's Rice Stadium Moon Speech," *NASA.gov*, 12 September 1962, http://er.jsc.nasa.gov/seh/ricetalk.htm.

36. "I want Americans to win the race for the kinds of discoveries that unleash new jobs—converting sunlight into liquid fuel; creating revolutionary prosthetics, so that a veteran who gave his arms for his country can play catch with his kid; pushing out into the Solar System not just to visit, but to stay." Pres. Barack Obama, "State of the Union Address – January 20, 2015," https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015.

37. Some of these steps were proposed in the president's FY 2014 budget. See "Fact Sheet: A Better Bargain for the Middle Class: Jobs," The White House, 30 July 2013, http://www.whitehouse.gov/the-press-office/2013/07/30/fact-sheet-better-bargain-middle-class-jobs; and Advanced Manufacturing National Program Office, "NNMI [National Network for Manufacturing Innovation] Snapshot," *Advanced Manufacturing Portal*, 2015, http://manufacturing.gov/nnmi.html.

38. Ibid. Previous studies have indicated that the outcome of such an initiative could be the creation of a set of innovation hubs, as industry selects schools to specialize in their requirements and then fund scholarships to these locations to produce their future workforce.

39. Muro, Rothwell, Andes, Fikri, and Kulkarni, *America's Advanced Industries*, 1–3. These researchers count among the advanced technology industries all those in which research and development exceeds $450 per employee; foremost among these industries is aerospace products and parts.

40. Ibid., 3–5. In addition, the value added to the economy of those who are employed in advanced technologies is over $210,000 per person—more than any other economic sector.

41. "Statement of the Participants of the 2015 Pioneering Space National Summit," *NASA.gov*, 26 February 2015, http://www.nasa.gov/content/pioneering-space-national-summit-2015/.

42. Stephen Trimble, "Full ADVENT Engine Tests meet Fuel, Heat Goals: GE," *Flightglobal* (web site), 21 January 2015, http://www.flightglobal.com/news/articles/full-advent-engine-tests-meet-fuel-heat-goals-ge-408182/. GE's latest tests show an improvement in engine efficiency of approximately 35 percent. Similarly, NASA's Environmentally Responsible Aviation program is looking at innovative concepts in propulsion that will not only reduce engine pollution but also enhance aircraft efficiency from both platform and propulsion standpoints. See "Environmentally Responsible Aviation Project," *NASA.gov*, 7 August 2015, http://www.aeronautics.nasa.gov/iasp/era/index.htm.

43. NASA, the Air Force Research Laboratories, and the Boeing Phantom Works are testing a blended-wing body demonstrator, the Boeing X-48C. Michael Braukus, Gray Creech, and Tom Koehler, "Release 12-259: Transformed X-48C Flies Successfully," *NASA.gov*, 7 August 2012, http://www.nasa.gov/home/hqnews/2012/aug/HQ_12-259_Transformed_X-48C_Flies.html#.VQikCf50zxg. NASA's ongoing efforts continue to develop a new aircraft design that is much more fuel efficient and will likely achieve success in the near term.

44. While not an exhaustive list, companies such as Cessna, Piper, and Gulfstream are among those whose aircraft size may be optimum for small, nascent emerging markets. In the area of utility aircraft, companies such as Air Tractor may be a key supplier of utility and agricultural aircraft to these same parts of the world.

45. Olga P. Popova, Peter Jenniskens, Vacheslav Emel'yanenko, Anna Kartashova, et al., "Chalyabinsk Airburst Damage Assessment, Meteorite Recovery, and Characterization," *Science*, 342, no. 6162 (29 November 2013): 1069–73, http://www.sciencemag.org/content/342/6162/1069.

America's Machiavelli Problem

Restoring Prudent Leadership in US Strategy

Damon Coletta and Paul Carrese

Abstract

The end of Pres. Barack Obama's first term coincided with the five hundredth anniversary of *The Prince* (1513) by Niccolò Machiavelli. Some analysts combined these milestones and praised the president's foreign policy performance as heeding Machiavelli's classic advice: the president, impressively, adapted lessons of *The Prince* in crafting a realistic and prudent first-term grand strategy. Avoiding major war or new commitments, he never agonized over legal or moral niceties when focused violence was necessary, as in the operation to eliminate Osama bin Laden. In the second term, however, the president's highly cautious strain of defensive realism fared poorly—a verdict upheld by commentary from his former lieutenants. This unwelcome turn of fortune calls into question whether strategy pundits and scholars correctly interpreted Obama's overcorrection, much less Machiavelli's imprimatur, during the first term. Contrary to the administration's recent justifications for "common sense" risk avoidance, Machiavelli's sophisticated notions of realism and statesmanship demand a strategy that more astutely blends daring and caution, including the articulation of an ambitious public purpose for US power. A genuinely prudent strategy, according to Machiavelli, accepts some near-term military risk to do good—and do well—in the long run.[1]

Damon Coletta is a professor of political science at the USAFA. He coedited *American Defense Policy*, 8th edition (Baltimore, MD: Johns Hopkins University Press, 2005) and *Space and Defense Policy* (New York: Routledge, 2009). Additionally, he is editor of *Space & Defense* journal, at the Eisenhower Center for Space and Defense Studies, USAFA.

Paul Carrese is a professor of political science at the USAFA. His most recent book is *Democracy in Moderation: Montesquieu, Tocqueville, and Sustainable Liberalism* (New York: Cambridge University Press, forthcoming March 2016). He is also coeditor of *American Grand Strategy: War, Justice, and Peace in American Political Thought* (Baltimore, MD: Johns Hopkins University Press, expected 2017). His essays on American grand strategy have appeared in *Orbis* and *The American Interest*.

✳ ✳ ✳ ✳ ✳

In strategic studies it is said that generals tend to fight the last war, and scholars, too, tend to grasp meaningful patterns and overarching solutions only as problems pass into history. So it was with Michael Ignatieff's 2013 article "Machiavelli Was Right," which favorably compared President Obama's first-term foreign policy with classic ruthlessness, given presidential readiness to violate the sovereignty of nominal allies in prosecuting Islamic terrorists.[2] Scholars who praised Obama's early policies, as the right strategic balance between using power and evading quagmire wars into which his predecessor dragged America, now share Ignatieff's fate of offering too tidy a solution to the previous problem of international hyperactivity and overextension. Pres. George W. Bush's critics, who became President Obama's defenders, crowded underneath a very big tent of "strategic realism," but the larger pattern of Obama's tenure clearly is one of committed restraint, not Machiavellian power politics.[3]

Machiavelli's place in history as a leading political thinker has been used to justify the current strategy of American retrenchment. But, a more balanced appreciation of Machiavelli would actually help American statesmen recognize the *costs* inherent in this policy. A Machiavellian perspective would judge that President Bush was imprudent in implementing his ambition for American power, but we have been wrong to assume it therefore endorses a reaction of having too little ambition. Ignatieff drew a deceptive conclusion from a favorable comparison of Obama in his first term and Machiavelli: success in the turbulent post–9/11 world required American statesmen to learn they "should not care" about how the use of force related to liberal ideals. Force was an instrument with material not moral consequences, and it therefore should be used to dispatch irreconcilable enemies like Osama bin Laden as cheaply and efficiently as possible. This validation, though, was not the correct reading of Machiavelli. Moreover, it paved the way for ill-conceived, less-effective strategic withdrawal.

President Obama's seeming string of first-term successes, along with praise for his toughness, faded as America and its chief executive encountered severe turbulence shortly after "Machiavelli Was Right" appeared. Machiavelli ultimately is correct about many things amid the geostrategic reality of America's constrained resources; however, the reasons,

contra Ignatieff and crucial for candidates and citizens to consider before a new commander in chief takes the helm in 2017, have more to do with seeing the danger of the American prince *not caring enough* to venture for strategic gains.[4]

After its recent lurching from one extreme to another, it is possible to find a sober middle course for American foreign policy. However, this will require recovery of principles that find a genuine balance between serving our ideals and employing the power needed to safeguard them.[5] Notwithstanding the administration's protestations of strategic realism, Machiavelli strongly opposed simple formulas to avoid war; rather, his cases and lessons inform the prudent judgment needed in given circumstances. His counsel is not so alien to America's tradition of accepting and coping with the moral burdens and material costs of wielding power in a dangerous world. Today, Americans must consult Machiavelli with care. As the United States enters the next presidential campaign and public debate begins over the strategic direction of American foreign policy, the country should transcend its present discourse on Machiavelli. *The Prince*, in other words, should not be oversimplified to exonerate either crusading belligerence or Panglossian minimalism in American strategy. Machiavelli instead ought to enlighten our strategic debates, helping us account for—rather than shade—the *calculated risks* democratic leaders must take to secure the national interest.

To show how this classic work relates to recent American strategy—especially to understand how the United States has lost strategic balance by overcorrecting from massive ambition to retrenchment—we place foreign policy in the context of grand-strategic thinking. We follow several recent works in defining grand strategy as the overarching conception that guides a rigorous calibration of ends and means that serve a state's view of international affairs and its place in the global order. Policy responses to individual crises are shaped and subsequently interpreted through a broader conception of global order conceived by grand strategy. When policies fail, this suggests problems at the root level of grand strategy—the deeper or higher orientation of policy.[6] Results now rattling world opinion and policy gambles premised upon war-avoidance seem just as likely to produce disappointing results and indicate a need to revisit our fundamental understanding of grand strategic principles.

Consulting Machiavelli to Diagnose America

America's miscomprehension of Machiavelli's advice in *The Prince* is of greatest concern to political leaders and their counselors, but it also matters to "we the people," who, under the Constitution, must hold leaders accountable. The commander in chief's extraordinary powers notwithstanding, in national security affairs and in other aspects of national life, Americans get the leadership they deserve. As a diplomat and organizer of militia for the Florentine Republic at the turn of the sixteenth century, Machiavelli recognized this pattern. In fact, he faced dilemmas of grand strategy surprisingly similar to those confronting America's Founders a few centuries later. Machiavelli sought a new kind of prince who could unite the principalities and republics of a divided (and conquered) Italy. A Machiavellian grand-strategic perspective advises a balance of hard power and diplomacy and is wary of overreliance on one versus the other. Likewise, American statesmen, led by George Washington, sought to galvanize elite and public opinion to unite querulous petty states into a *novus ordo seclorum*, "new order for the ages." There was much idealism—a sense of moral truth—motivating America's Founders, but they also adopted Machiavelli's hard insights and his regard for experienced judgment. They consulted the Florentine in direct study and also through the Enlightenment writers who had moderated Machiavelli's new doctrine of executive power. The American presidency is one product of this moderating of Machiavellism: a single prince, as commander in chief and master strategist, but tamed by a legislative branch sharing the war power, a Senate sharing many foreign affairs powers, and a requirement to be elected to a fixed term (not to mention threat of impeachment).[7]

America's robust sense of its exceptionalism always has included a blend of realism and idealism.[8] This mostly has served it well, supplying motivation for individuals to pledge their lives, fortunes, and sacred honor for the good of the republic. The sense that America stood for universal ideals—but also for the right to defend both its interests and ideals—fixed legitimizing purpose to US power as it expanded and eventually dominated. Still, American exceptionalism also encouraged statesmen to ban Machiavelli from its national narrative and traditions. We tend to refer to Machiavelli mostly as the Renaissance popes did—a teacher of evil—and neither we nor they have fully understood the disgraced bureaucrat.[9] His advice, to be "devious and ruthless rather than

honorable and fair," would undermine our claims to exceptionalism, defile the foreign policy legacies of presidents like Washington, Abraham Lincoln, and Franklin Roosevelt, and condemn future American leaders to be no better than the self-serving European princes in Machiavelli's time.[10] Realist international relations theory that influenced American strategists in the twentieth century hid its debt to Machiavelli and instead emphasized roots in Thucydides and Hobbes, borrowing liberally from rationalist cost-benefit analyses developed by contemporary economists.

Unfortunately, as the theologian Reinhold Niebuhr admonished after World War II, American exceptionalism can too easily metastasize into a reflexive confidence that moral superiority underwrites military superiority—the happy fallacy that right makes might.[11] In denigrating Machiavelli, even as they conceded after five hundred years that he is "too smart to ignore," America's political class failed to comprehend how much his advice to the new modern breed of rulers could help their republic in a difficult time, perhaps just one or two false steps from hegemonic collapse.

Counselors to President Obama understandably emphasized the rhetorical appeal of Machiavelli's astuteness and flexibility on moral norms for a strategy of rebalancing or retrenchment. American exceptionalism as the world-enforcer of liberal ideals, under this customary interpretation of *The Prince*, is a stupid extravagance. A president must instead appear to be good to the voting masses at home and allies abroad but never shrink from violence or betrayal of ideals when necessary to secure the state. These points are well taken *qua* conventional Machiavellism, but we suggest this is a misreading of Machiavelli's text and is, moreover, not what America needs to hear amid our post–Cold War confusion—regardless of what many elites and voters might prefer to hear.

Prodigal Grand Strategy of Restraint

President Obama's first term seemed to strike a balance between liberal ideals and the realistic need to use force in some circumstances. In his strategic rhetoric, he tempered invocations of international law and denunciations of his predecessor's unilateralism to reveal a Machiavellian side: both fox and lion. The new commander in chief's Nobel Peace Prize acceptance speech, delivered less than a year after his inauguration,

began "by acknowledging the hard truth," describing force as sometimes both necessary and morally justifiable.[12] He reinforced this message by retaining the thoroughly realist Robert Gates as secretary of defense, authorizing the troop surge in Afghanistan, dramatically extending drone warfare in the US Central Command's area of operation, and expanding strikes by special forces—including the raid on Osama bin Laden in Pakistan.

Even with significant Democratic losses during the 2010 midterm elections, foreign policy remained a successful arena for the president. Some achievements were diplomatic, including Senate ratification of a New Strategic Arms Reduction Treaty to reduce nuclear weapons, the seemingly productive reset with Russia, the shepherding passage of a new Strategic Concept for the North Atlantic Treaty Organization (NATO) after Afghanistan, and the nuclear negotiations with Iran (accompanied, in apparent Machiavellian *sang-froid*, with diffidence about the 2009 Green Movement and Iran's brutal suppression of it). Meanwhile, drone warfare decimated al-Qaeda leadership in Pakistan and the Arabian Peninsula. In late 2013 Ignatieff could write that Obama's success derived from a Machiavellian capacity not to overthink the human cost or moral implications of using force—or of refusing to intervene (as in Iran or Syria). The candidate of "Hope and Change" had internalized Leslie Gelb's interpretation of *The Prince*: "Power is power. It is neither hard nor soft nor smart nor dumb."[13] Only the people who allow politics at home to cloud their common sense abroad can be dumb.

However, by 2014 many of Obama's victories turned to ashes. Relations with Russia fell to Cold War levels, not least given the Russian invasion of Ukraine. Libya fell into anarchy after America's partial engagement then immediate military disengagement. The progress salvaged in Iraq disintegrated after America's complete military withdrawal. Equivocation in Syria, Central Europe (pulling our missile defense sites from Poland and the Czech Republic), Ukraine, and Egypt encouraged enemies and discouraged friends. Finally, the promise of a new era of free trade in the Pacific yielded to deadlock and acrimony—not least, regarding China.[14] Friends and adversaries alike perceived the proposed American "rebalancing" to Asia as really just a pivot away from the Middle East, because when coupled with cuts in defense spending and global military posture, America's presence in Asia was at best static in the face of Chinese territorial provocations and at worst a relative decline. Amid

many conventional commentaries on these reverses or doldrums, with Obama supporters arguing that they paled in comparison to avoiding the costs of another war, retired US diplomat Roger Harrison sought a diagnosis of deeper causes through an imagined dialogue between Machiavelli and Obama. "Your mistake, if you will excuse my frankness," said his Machiavelli, "was to judge your former success as a function of virtuous leadership rather than the gift of fortune."[15] This warning against complacency, or reliance upon simple doctrines, captured the complexity and wry sophistication of Machiavelli better than Ignatieff's shopworn teacher-of-evil meme.

In his first term, Obama sometimes was a ruthless prince and generally was a fortunate one. Bin Laden and his Pakistani hosts became careless. Old autocrats vanished with the Arab Spring, and others—particularly Syria's Bashar Assad—seemed fated to follow. Russia apparently acquiesced (grudgingly) to the EU and NATO push eastward and saw common ground in keeping nuclear weapons out of Iranian hands. All this was fragile to the point of being a hypnotic mirage. The Obama administration nonetheless deemed it the result of just the right mixture of violence, prudence, and foresight. Senator Obama's campaign denunciations of overreliance on force and American exceptionalism seemed vindicated, while inexhaustible strategic patience and flexibility were the new virtues. In fact, the new president was just as wedded as his predecessor to the infallibility of strategic dogma and now, in quite un-Machiavellian fashion, failed to see Nemesis, the classical spirit who lies in wait for self-satisfied statesmen.

Machiavelli knew that evil deeds or cunning diplomacy by themselves cannot grant a prince immunity from ill fortune or the turbulence of human affairs. The real measure of a prince, at the precarious summit of power, is his ability to overcome fortune with a blend of calculation, strength, cunning, and decisiveness that he called princely *virtù*. An executive must strive to rule fortune rather than be ruled by it. Nowadays, Obama's critics accuse him of having no strategy at all, merely reacting to unanticipated events rather than dictating the pace of change.[16] Indeed both friends and enemies, at home and abroad, sense this as not the wisdom of strategic patience but incapacity. The result, as Machiavelli predicts, has been a run of foreign policy disasters—and, with the Iran deal, further retrenchment from forceful leadership and forward presence in supporting the liberal global order, even while disclaiming any such intent. In domestic terms,

the president's negotiating approach (to sideline Congress and accept weak final terms) further polarized relations with Congress; internationally, the high price included his cautious stance toward the strategic and human disaster in Syria—now spilling into Europe—and an emboldened Iran and Russia as geopolitical actors.[17]

Machiavelli offers hints as to why such things will happen: the habitually cautious prince learns, as does the habitually impetuous one, that "if the times and affairs change, he is ruined because he does not change his mode of proceeding."[18] This is especially the case when one's ways seem to have been successful, for example during the first terms of George W. Bush and Obama. Beyond this are sins to which rulers seem heir. *The Prince* especially advises care in selecting counselors: a ruler should choose "wise men in his state . . . to speak the truth to him . . . [and] ask them about everything."[19] Obama seemed to heed this at first, with the appointments of Robert Gates, Hillary Clinton, and David Petraeus among others. Memoirs of that period tell us that debate among these advisors often was heated, just what a prudent executive should desire.[20] At the inauguration of his second term, however, the president chose to refurbish his foreign policy team, appointing insiders whom he liked, trusted, and, not incidentally, dominated as their chief patron. Are these the "flatterers" whom Machiavelli describes as a "plague" to any prince?[21]

However, the deeper issue for American leadership is that much conventional advice on power, the summing up or refinement of Machiavelli's wisdom, has been flawed. Despite profuse analysis for the quincentenary of *The Prince*, a subtler reading of Machiavelli still is needed, coupled with cautions about how American statesmen can consult his works.

Interpreting Machiavelli: A Teacher of Prudence

The Prince does employ shocking irreverence. By assaulting readers with story after story of historical deception, betrayal, and murder as elements of a new princely *virtù*, Machiavelli seemingly wanted to bludgeon potential converts into accepting the necessity of evil, or "dirty hands," to secure the state. Yet, in distilling Machiavelli to such an essence, the experts bypass complexities not easily captured for a presidential memo. The allure of his iconoclasm, his confident astuteness, leads us to overlook enduring tensions in his counsels.

Contrary to partisan attacks on President Obama's deliberative (critics say halting) foreign policy, it is unlikely that after six years in office the commander in chief lost all determination or unlearned his competence. Rather than forget the lessons of Machiavelli, it is more likely the young president, with little foreign policy experience when he entered office, never learned them well enough. For that, we should not blame the student alone but also his several teachers, broadly construed—the policy advisers (*consiglieri*) and scholars who have interpreted Machiavelli for the age of the *Pax Americana*. It is not so much that Carnes Lord, Leslie Gelb, and most recently Michael Ignatieff are dead wrong in what they wrote.[22] It is that more needs to be said because such counsel infantilizes American princes by glossing over their most demanding strategic dilemmas—those pitting US interests against our ideals. The conventional advice resolutely adheres to *one side* of a profound debate about what Machiavelli really meant in his primer for a new, distinctly modern brand of political leader.

Two Contemporary Schools on Machiavelli

The predominant view has roots in Friedrich Meinecke's post–World War I study, *Machiavellism*, but was revised by Leo Strauss's *Thoughts on Machiavelli* (1958) and the essays by Harvey Mansfield that it inspired (*Machiavelli's Virtue* [1996]).[23] For these scholars and for most readers, Machiavelli's brutal experience in the service of Florence—as it declined militarily and politically from destructive competition among Italian city-states, a wave of imperial intrigue from France, and the repressive protection of the Medici family—spurred him to unprecedented boldness. Mansfield sees Machiavelli's greatness in his aim to be Prince of princes, conquering future rulers and subjecting them to modern orders in the only way open to him: inventing a radical but attractive philosophy. The universal struggle to found the best regime on earth now would have a fair chance of succeeding once Machiavelli, with nothing left to lose, hazarded the master stroke. Reason would free politics "from the superintendence of Christianity."[24] Still, the astute prince would not do evil uniformly, in a doctrinaire way, for this would provoke blowback and be ineffective; rather, in his subtle teaching, "it is necessary to a prince . . . to learn to be able not to be good, and to use this and not use it according to necessity."[25]

In the introduction to his translation of *The Prince*, Mansfield conceded the strong temptation to avert one's eyes from the stark truth and to reach for excuses to downplay Machiavelli's blasphemy, but, he insisted, *The Prince* ultimately was more interesting and significant if we encountered its spirit of *realpolitik*—a politics without God. This is just one of several themes in Mansfield's account of Machiavelli's intent and legacy, but it has enthralled a new breed of counselors who would tap Machiavelli to enshrine a certain prototype of American statesmen. Lord, Gelb, Ignatieff, and many others in relevant periodicals of the American foreign policy establishment must keep Machiavelli interesting for their soft, blinkered, largely Christian audience whose instinct moves them to go about politics without blemishing either the nation's founding values—freedom, equality, and justice through the rule of law—or the commandments of God. In this strategic realism influenced by the Straussian interpretation, what is interesting about Machiavelli is his ruthless, fearless iconoclasm in speaking truth about power to Power. These Machiavellian counselors to America would upend our customs and courtesies of diplomacy, slap us across the face, wrench us away from hopeful reverie, and batter us with shocking, brutal, yet enticingly risk-free requirements for maintaining our position in global affairs.

However, a major problem with this use of Strauss's and Mansfield's stark renderings of Machiavelli is that Americans cannot live long in a nihilistic, code-red condition the teacher-of-evil recommends. To pick on the current Machiavellianists once again, American princes are most unlikely to look upon the Constitution as mere parchment; they will not evaluate costs and benefits of US military intervention according to commonsense criteria if said criteria ignore indignities to human liberty or political equality. They might learn, as Ignatieff suggested, to not care about morality in the use of power in a moment of weakness but eventually will unlearn this lesson, returning to themselves and addressing their conscience.

At the risk of excusing Machiavelli but with the intended reward of kindling American interest in his lessons for grand strategy, we consider the thinking of Maurizio Viroli (*Redeeming the Prince* [2014]).[26] Viroli's rejoinder to Mansfield's stark witness about Machiavelli's new prince is just as shocking but far more appealing for an American audience. Ingeniously, Viroli drew on the same passages from *The Prince* and co-opted Mansfield's language but still argued a diametrically opposed case. Viroli

wagered that seducing heads of state away from Church morality and evangelizing them with a new covenant—no-nonsense rules for exercising power over men—implied neither revenge for a discarded secretary of Florence nor even the ambition to be Prince among princes. Machiavelli did not merely wish to convert future rulers to his philosophy; for Viroli, *The Prince* only made sense if Machiavelli sought to *redeem* them. To redeem is to save, to bring someone back from disgrace or certain death, so they may live (and strategize) again within sight of God. Rather than destroy religion, Viroli sees Machiavelli surveying its practical limits in this world but still invoking it to rescue Italy from the cataclysm brewing among anachronistic empires, the corrupt Catholic Church, and the vulnerable system of republican states in the sixteenth century. It was the independence and prosperity of those free states that most concerned Machiavelli in his final chapter, the "Exhortation to Seize Italy and to Free Her from the Barbarians."[27] Machiavelli's closing argument is seen as the key to the entire book and his new philosophy: Italian states, well-ruled and at peace with one another, could, "with God's help," bring about justice through "good political order."[28]

If Viroli is correct that there is a viable Christian republican reading of Machiavelli, then, suddenly, Machiavelli's whisper to the new breed of princes is both relevant and tantalizing to each generation of free American citizens who superintend their president. The closing exhortation to unite the miserable, disoriented republics of Italy under one flag becomes, however unlikely it might seem, a hymnal for the God-fearing Founders who dared to transform the United States from thirteen miserable, jealous republics. As John Jay paraphrased Shakespeare in "Federalist Paper, No. 3," in *The Federalist* "I sincerely wish that it may be as clearly foreseen by every good citizen, that whenever the dissolution of the union arrives, America will have reason to exclaim in the words of the Poet, 'Farewell: A long farewell to all my greatness.'"[29] For the American Founders as for Viroli's Machiavelli, the humiliation of Italy's protorepublics by European great powers after the fifteenth century is an object lesson.[30] There will ever be inadequate justice, insufficient freedom, and too little hope of happiness without *virtuous* statesmanship. This professional quality must look to immediate survival and, beyond, to the dignity of the greater republic. Machiavelli would grasp that America's enormous strength is founded on the enthusiasm of its people, and the foundation is ruined once people come to understand their

government, which derives its authority from consent of the governed, is merely carrying out the devil's work. Even if our prince, laboring under the Constitution and identifying with American political culture, responded to Machiavellian seduction—abandoning archaic sentimentality about the arc of history to embrace modern, scientific management of affairs—could any president (or adviser) long defend such an alien cost-benefit calculus amid domestic skirmishes and inevitable setbacks abroad without engaging his heart, that is, without ever being able to love this philosophy?[31]

Yet, how can Americans hold onto their ideals at the same time they sanction forceful, sometimes ruthless, policies around the world under the obligation to answer threats from other states? Of course, Samuel Huntington and other students of politics tackled similar questions in the decades after World War II, when the United States donned responsibilities and claimed the license of a world power.[32] In the aftermath of 9/11, as network-based actors rose alongside conventional adversaries of the United States, the controversy between pursuit of transcendent ideals and material interests flared once again.[33]

Without defining justice for sixteenth-century Europe, much less for today's United Nations, Machiavelli does provide partial guidance from across the centuries. Perhaps because of our newer technology and subsequent experience we doubt this could be so; however, we would do better to doubt our sense of progress or superiority. The extreme violence endorsed in *The Prince* indicates that for Machiavelli no moral code can stand unscathed against forces of necessity or threats to state survival. Still, Machiavelli clearly condemned cruelties "badly used." If the butchery grew with time, out of proportion to its utility for subjects under the prince's sway, then there was no "remedy for their *state* with God (nor) with men" [emphasis added].[34] Such passages remind readers that whether Machiavelli thinks God is actually present, he knows the possibility exists in the minds of most citizens. All peoples grant that, for necessity of civil order on earth we must at some point accept the authority of one prince or another. Nonetheless the moral judgment of society *does* matter for preservation of the state—and for the prince. Therefore, rulers must hazard this judgment by entering into evils—but only when necessary. Moreover, the people are a crucial judge of what truly constitutes necessity versus inexcusable extremes. Thus, Machiavelli took pains to instruct statesmen on an economy of violence or, as

Markus Fischer argued, on how to comprehend and employ their well-ordered license.[35]

Opening the American Mind: Whose End Justifies the Means?

Fischer's prudential, calculating Machiavelli enriches our understanding of the most famous passages in *The Prince*, thereby connecting this classic work closely, and more fruitfully, to American foreign policy traditions. In chapter 18, "In What Mode Faith Should Be Kept by Princes," there are seminal lines often translated in the popular imagination as "the end justifies the means."[36] Even as sophisticated a reviewer as Ignatieff seemed to reduce this subtle chapter to a sentiment: Do what you want to achieve your end; particularly in the hostile atmosphere of national security competition, if he who cares about morality or the end of history pauses to reconsider, and he who hesitates is lost, then a chief of state must learn not to care. We respond that the phrasing of the original Italian text invites a subtler interpretation.[37]

When these (in)famous lines appear, in the final paragraph of that chapter, Machiavelli is explaining why subjects or citizens will not hold the prince to account once he breaks faith by deviating from accepted moral norms. In the actions of men, Machiavelli wrote, where there is no authoritative tribunal to try whether certain behavior is criminal, "one looks to the end."[38] This is a fair rendering of *si guarda al fine*, but it is worth noting that Machiavelli's choice of the verb *guardare* also has connotations of watch, protect, and account for. Citizens, benighted though they may be, feel themselves entitled to protection and defense provided by the state—as Machiavelli notes. Their desire for security influences their verdict, perhaps more self-interested than moral, on a prince's transgressions. Such would certainly include, for Machiavelli, prudent transgressions against dogmatic, politically popular formulations of strategic realism.

These implications of *guardare* are consistent with Fischer's moderate interpretive approach. Given the prince's duty and interest to maintain the state, the ruled population will naturally grant some license to their leader—their enforcer of order and champion of national reputation—so he may make exceptions to right action in their mind *for the welfare of the state* without thereby soiling his appearance, his personal reputation

for goodness, or his moral authority in the eyes of the many. As Fischer implies, this permissiveness, or room for maneuver, is not unlimited. It requires skill to be used properly and is, therefore, well-ordered license.

Machiavelli is addressing a new prince's understandable concern about losing public approval and risking contempt from the governed. *Si guarda al fine*, "the end is looked to," urges the reader to inquire as to whose end and who is doing the guarding. In the actions of all men, and most of all of princes (who act in the name of the state), the end is watched over. Yes, but *whose* end? For centuries, most Americans have assumed this must mean the prince's desire. Mad George III, for example, as portrayed in the Declaration of Independence, usurped the colonists' natural rights and thus was indicted by Americans—basically, for turning Machiavellian.

Machiavelli, though, wrote about acquiring and maintaining valuable territory, not losing it in colonial rebellion. Did the king lose for following Machiavelli? Intriguingly, for the alternate interpretation—"the end is looked to"—there is no need to be specific about whose desire comes first. The unity, security, and glory of the state are, after all, in the interest of everyone in the population, which comprises (as Machiavelli explicitly states in this crucial paragraph of chapter 18) the common citizen (*molti*), the elite (*pochi*), and the head (*principe*). In his grammar as well as his logic, it seems, Machiavelli sought to master centrifugal forces threatening to dismember any state, even more a republic, which must labor under the challenge of *e pluribus unum.* Who, then, attends the end if it is the security and greatness, or reputation, of the state? This "end," of course, is guarded by all classes, though by different modes of reasoning according to their capacity, as Machiavelli reported. So let a prince bring a people inhabiting their territory, their home and hearth, under his will and thereby maintain the integrity and dignity of the state, and the means will always be judged honorable, and each one (*ciascuno*), each citizen, regardless of whether they belong to the many or the few, will give praise.

Taken in context of the logic of necessity and an economy of violence, unsavory methods to save the union will not be held against the prince. These same actions, though, should they leave the state less secure—or morally contemptible given inexcusable violence—may ruin him. Machiavelli's counsel on acquiring and maintaining the state alerts us that well-ordered license leaves princes a daunting challenge: how to pursue

interest and some sort of justice at once. This is hardly a counsel for prudence as mere strategic caution, as risk-averse and parsimonious use of power in a dangerous world—especially for a state, like America, animated not only by glory but by concerns for justice at home and abroad.

Time to Adapt and Modify *The Prince*

The predilection in US broader strategic culture to caricature Machiavelli and discount his relevance for a liberal republic has contributed to a recent string of policy failures. Both allies and adversaries now perceive US relative decline since the troubled interventions in Afghanistan and Iraq and the way each was handled across two presidential administrations. The global financial crisis triggered by the United States in 2008 also has damaged the standing of the American model. The rise and fall of President Obama's foreign policy and a steep decline in public opinion supporting the administration's framework (built across two *National Security Strategy* documents published in 2010 and 2015) prompted a torrent of criticism, including from the president's own lieutenants.[39] The Joint Comprehensive Plan of Action (JCPOA) on Iran's nuclear program, premised upon a war-avoidance strategy and American retrenchment, could appear to ratify perceptions (and reality) of American decline since it concedes precisely what, for decades, bipartisan policy has sought to deny: a credible Iranian nuclear weapon capability.[40] However, neither Obama nor Bush before him deserve all the blame for America's fitful performance in the past two decades, especially when they received inadequate or narrow-minded strategic advice.

President Obama's recent articulation of grand strategy—in remarks to the press and in the administration's 2015 *National Security Strategy*—echoes the old-line realists.[41] The United States does and will continue to do everything within its power to win engagements in defense of its values. However, when there is nothing on the table worth fighting for in Syria, Iraq, Ukraine, Libya, Yemen, or the South China Sea, or in accommodating Iran, despite it being the world's leading state sponsor of terror, then non-intervention and imperturbable caution regarding other powers is the order of the day. The president once summarized this in a polite version: "Don't do stupid stuff."[42] This maxim supposedly solves several problems. It follows Gelb's advice to see costs as they are rather than as politicians wish, and it echoes Ignatieff's advice that

regardless of moral duties and international legal norms, if a military engagement might bring disaster—in Afghanistan, Iraq, Iran, Libya, Syria, Mali, Ukraine, or East Asia—then it would be stupid to try. It is better not to care. When the United States learns not to care so much, moral and legal principles and the verdict of history are not burdensome. They do not hamper clandestine operations like those used to hunt down and kill bin Laden; at the same time, brush fire conflicts never demand sacrifice. Indeed, risky escalation and costly fighting for a cause are someone else's problem. No matter how badly world affairs trend today, no matter the rise of illiberal and autocratic powers, even terrorist powers, at least we leave behind the era of the preceding prince when America *did* do stupid things and incurred steep costs as a direct result.

Nonetheless, a strategic formula so tidy and politically expedient for the second term was bound to distort rather than channel Machiavelli. The policy mining of *The Prince* and convenient refinements of the realist brief elide fundamental controversies about Machiavelli's philosophy that scandalized Renaissance Italy and early modern Europe. These controversies simmer underneath the world headlines blaring about globalization or the US pivot to Asia. American statesmen and their counselors should remember that scholars are divided on strategic realism. Was Machiavelli a teacher of evil or a tough-minded redeemer for Italy—and, by extension, all republics? Was he anticipating twentieth-century nihilism, or did he long for a return to republican liberty? Many read the deceptively accessible arguments of *The Prince* as part of their strategic education, but few discern a seminal philosopher with deep and challenging guidance for American grand strategy.

Strategic Realism and American Prudence

As we enter another presidential campaign season, we caution American princes and their counselors. In an era of doctrinal conflict for international relations theory, with armed trenches dividing realists, liberal internationalists, and constructivists—and similarly doctrinaire polarization among camps of Republicans versus Democrats and interventionists versus isolationists—we can profitably consider that Machiavelli counseled not rigid extremism but rather intellectual moderation about power and politics.

Seeing Machiavelli's moderation does not mean we pardon his immoderate stance toward sacred honor, religion, or ethics. Unless our leaders (elected politicians and their counselors) would change America's character, the United States cannot blithely descend, under the guise of strategic realism, to astute immorality—even if it means US leaders will accept greater risk to themselves and their country's fortunes than Machiavelli would. The extra burden growing out of the Founders' constitutionalism requires that the prince must debate or test his policies and his grand strategy with Congress, and this comports with Machiavelli's counsel for balance. The salutary moderation we take from Machiavelli means embracing the competing principles and tradeoffs rulers face. Circumstances are fluid, and the course of hazards always shifts. Formulaic advice from one academic school or another, though easiest for a prince to imbibe and counselors to offer, is suspect—for Machiavelli and for us five centuries on.

Yes, Machiavelli prized astuteness in grand strategy but never to a cautious extreme. Today's strategic realism jeopardizes the security and reputation of the American state just as extravagant use of force did before it. Republican princes as much as others must lead through *virtù*—a prudent faculty for consolidating state power while coping with the whims of *Fortuna*. An effective prince, in other words, cannot be predominantly man or beast, and when beast, the prince must don the attributes of both fox and lion.[43] Dilemmas of the world—and an American executive in the twenty-first century must think globally—always demand adept balances. The mostly-overlooked tensions in Machiavelli's thought thus counsel skepticism about formulas that eliminate the need to place bets as a leader to take bold stands for enlightened interest or principle rather than wait for fortune (or adversaries) to decide. Even the most powerful rulers cannot stand pat at each individual crisis, imagining that, somehow inert, it must begin and end in total isolation from future bargaining. American presidents, too, must seize the initiative and accept risk to advance or protect interests, power, and ideals. Machiavelli scoffed at temporizing to avoid problems. Had Machiavelli heard of such policies or strategies as strategic restraint and offshore balancing, or alternately preemptive war and domino theory, he would have recognized how a prince obeisant to public fears could follow any one of them to perdition. He would be particularly dismayed, then, that his argument in *The Prince* is twisted to compound the hidden but real dan-

gers of guileless strategic withdrawal. Machiavelli counseled it is better to be feared than loved, but it is best to be both (chapter 17), which in democratic politics will require of the elected leader a healthy amount of dash. Today, as in international politics before, *Fortuna* ultimately favors the bold.[44] For the president's second term and beyond, this requires a man or woman of laws who is sly like a fox yet knows when to keep opponents at bay by acting the lion.

Machiavelli's complex balancing of roles required a defense of evil, thus moral agnosticism, which admitted an economy of violence and impious acts. If such dirty deeds are either shunned or indulged it would mean the ruin of a prince's political capital, the long-term foundation of his authority. Machiavelli's clear-eyed analysis of power and interest led progeny in Europe and America to formulate many refinements and subvarieties of amoral realism.[45] Our moderate reading of Machiavelli challenges the facile and too common realist approach. Just as not all *virtù* is common sense (e.g., it is not so easy to know when to be bold), not all prudence fits neatly within doctrines. Prudent leadership in democracy demands artifice through a summoning of intellect in addition to armed force and superior will; in its Machiavellian form it recommends, as Fischer termed it, well-ordered license. The necessary ratio of fox to lion, of being loved or feared, is never clear in advance. That said, Americans must take Machiavelli in moderation, blending a human element with these base realities of global affairs, to be not just the eagle but to defend right as an eternal, transcendent objective: *novus ordo seclorum* in the Founders' Latin phrase.[46] Because this precludes a foreign policy of evil actions for sheer advantage, America must invest in extended deterrence, pay for global capability, and cultivate a willingness to accept risk in order to preserve alliances with other republics.

In response to spreading crises through multiple regions of the world, President Obama insisted that the astute baseball manager prefers "small ball" to recklessly swinging for the fences. There is in such strategic discourse and in the president's *National Security Strategy* a hint of *post facto* rationalization, of tunnel vision masquerading as prudence. Formulaic risk aversion actually discourages frank assessment of a fluid and interconnected security environment. Again, Machiavelli is apropos to resisting overcorrections in grand strategy: "It is found that one never seeks to avoid one inconvenience without running into another; but prudence

consists in knowing how to recognize the qualities of inconveniences, and in picking the less bad as good."[47]

Admittedly, any administration can easily dismiss critics in the gallery. Observers have the luxury and, in the United States, the freedom to chastise the executive for inaction in Syria, Afghanistan, Ukraine, Iraq, Yemen, or elsewhere, not knowing what consequences action would have wrought. Still, even the president's friends at home and abroad increasingly warn of disturbing *trends* in the words and deeds of his second term, and these criticisms have registered in the polls on foreign policy performance. Regardless of whether specific concessions in each instance were cheaper than fighting, the global series of diplomatic setbacks framed by the president's determination to avoid another American war instantiates for friend and foe the impression of an American executive overwhelmed, unable to anticipate threats, losing initiative and command. This mounting preoccupation in public as well as elite opinion, beyond any one tactical decision, exposes drift and confusion in US foreign policy.

It is hopeful, in a sense, that there is growing consensus that the tenor of current US foreign policy is extremely risk averse or immoderate. Again, contrary to conventional interpretations of realism, *The Prince's* counsel for nuance and a daring blend of offense with defense affirms rather than assuages such concerns. Negotiations, symbolic deeds, or partial sanctions will cost more and produce less diplomatic leverage day-after-day, compared to policies that force others to rebalance their strategic conceptions and strategic guidance that allows for calibrated risk of military operations abroad.[48] As events spiral out of control, the president's options will narrow and the price of war avoidance at each crisis will grow. He will impress no one at home or abroad with lawyerly presentations about what the United States did *not* do or sundry hypotheticals the country managed to sidestep thus, we can expect the enduring, churning pattern of world politics to swamp American exceptionalism. Lack of a viable candidate in our time to replace America as the leading crafter of international order buttresses Machiavelli's counsel against doctrinaire risk avoidance.

Any American executive who would lead the world must defend his previous ideas and avoid stupid mistakes, of course, but he also "needs to have a spirit disposed to change as the winds of fortune and variations of things command him."[49] As American fortunes in the world have

changed, the American executive has not adapted strategic realism, and the energy of the office has waned. Despite omens of violent change, threatening to destroy institutional structures of the American-led international order, the United States currently lacks the strategy and, Machiavelli might add, the spirit to restore its national security tradition of prudence in the presence of evil—of balancing power, legitimacy, and risk according to a principle of enlightened self-interest.

Conclusion: Toward Enlightened Self-Interest

Machiavelli's counsel for post–Cold War America might ultimately be that embracing strategic realism—if it means refusing good works, avoiding all risks, and never being good in order to keep from doing stupid things—effectively hands over perfect intelligence and initiative to a state's adversaries. There is no dignity, no successful diplomacy, nor ultimate security in such a cautious, hollow grand strategy. Acting effectively in a world of competing sovereign states *at times* involves hypocrisy, betrayal of ironclad commitments to principle, and taking enemies by surprise. Machiavelli pointed out that citizens who are worthy of securing will accept evils orchestrated by the prince if such evils are tied to the well-being of the state, but it does nevertheless fall to the prince to correctly anticipate when flexibility in tactics really is necessary. If the prince gets the balance wrong, shifting his stance too late or too early, he and the state will pay dearly.

If the United States hopes to realize its professed aim to lead and sustain a liberal global order, it can ill afford such strategic mistakes, and a fuller appreciation of Machiavelli would be particularly useful. While American strategy must continually temper his perspective, the United States would do well to heed Machiavelli's advice on gamesmanship and his disdain for rigid prescriptions either to act the gladiator at all events *or* to frame every crisis as a war hazard—a brush fire amid dry tinder to be extinguished or avoided at whatever price.[50]

Rather than instructing us to neglect moral constraints, act dishonorably, and become evil—a policy that would devour America's constitutional limits on government and eventually the state itself in a fever of nihilism—*The Prince* can be read to urge republican statesmen to think carefully about moral suasion and measure it accurately against competing dangers of violence, submission, or penury for the state. The commotion of

The Prince's 500th anniversary has receded, but those considering prospects for a Second American Century after 2017 have yet to properly recognize Machiavelli's deeper contribution. A prudent reading of Machiavelli, one that empathizes with princes rather than dehumanizing them or subordinating them to abstract theories of realism or idealism, would highlight the difficult judgments princes can expect rather than denying such burdens. Our view offers a more fruitful path for future American strategists and a more sober yet exceptionalist context for US foreign policy debates. In Machiavelli's republics as well as our own, a clear picture of enduring dilemmas tied to republican stewardship ultimately benefits the ideals *and* interests of the electorate, whose relationship with their chief executive is crucial to the state's power and influence. A more discerning basis for strategy would prevent our elites and the broader electorate from falling for the policy extremes of recent decades—in which we lurched from demanding a perfect defense to expecting too little of the presidency and America.

Consensus held in the last century that America would sacrifice to defend a cosmopolitan civilization as the best way to secure its interests while strengthening ideals of law and right as limits upon power, war, and ruthlessness. Now, we should recover strategic balance: calculating enough to survive the snares and monstrous threats of international politics, and cognizant of the tragic history of hubris in international affairs (our own included), yet retaining a larger purpose in the world to prudently guard the principle of liberty and justice for all. Enlightened self-interest honors principles of right and peaceful global order, now, as the best path to maintain our material strength and security for liberty over the long run.[51] In the turbulence of the post–Cold War era, coupled with increasing polarization and partisanship about foreign policy at home, we have lost our strategic compass for prudential balance, careening half-panicked from hyperactivity to the even less Machiavellian paralysis of small ball. A genuine dose of Machiavellian *virtù* tempered by American enlightened self-interest would help our next chief executive, as steward of the Republic, to lift US strategy without overinflating American commitment around the world. Riskier though it may be in the near term, Machiavelli would heartily approve if the next US strategy actively engaged fortune while pressing the commitment to a better Rome. SSQ

Notes

1. An earlier version of this article was presented at the ISSS-ISAC Joint Sectional of the International Studies Association and the American Political Science Association, Austin, TX, November 2014. The authors also draw upon an earlier collaboration with our colleague Dr. Roger Harrison on Machiavelli's relevance for current strategic debates.

2. Michael Ignatieff, "Machiavelli Was Right," *The Atlantic*, December 2013, http://www.theatlantic.com/magazine/archive/2013/12/machiavelli-was-right/354672/.

3. In addition to Ignatieff's 2013 essay, defenders of Obama's just-right recalibration include Fareed Zakaria, "On Foreign Policy, Why Barack is Like Ike," *Time*, 19 December 2012; Joseph Nye, *Presidential Leadership and the Creation of the American Era* (Princeton, NJ: Princeton University Press, 2013); and Barry Posen, *Restraint: A New Foundation for U.S. Grand Strategy* (Ithaca, NY: Cornell University Press, 2014).

4. Peter Feaver, ed., *Strategic Retrenchment and Renewal* (Carlisle Barracks, PA: Strategic Studies Institute, US Army War College, 2014), 1–6.

5. This is the larger theme of Henry Kissinger's *World Order* (New York: Penguin Press, 2014); American grand strategy, and the liberal world order it built and now should renovate, must balance ideals of freedom and legitimacy with realities about power and thus accommodation of other civilizations and great powers (e.g., 8–10, 232–335, 362–63, 367, 370, and 373–74).

6. For a related, but still distinct, analysis of the Obama policies and grand strategy, see Colin Dueck, *The Obama Doctrine: American Grand Strategy Today* (New York: Oxford University Press, 2015). For our conception of grand strategy and its priority for guiding and testing policy, we draw upon (among other works) Dueck; Hal Brands, *What Good Is Grand Strategy? Power and Purpose in American Statecraft from Harry S. Truman to George W. Bush* (Ithaca, NY: Cornell University Press, 2014); and William C. Martel, *Grand Strategy in Theory and Practice: The Need for an Effective American Foreign Policy* (New York: Cambridge University Press, 2015).

7. See Harvey C. Mansfield, *Taming the Prince: The Ambivalence of Modern Executive Power* (New York: Free Press, 1989), chapters 8–10 on Locke, Montesquieu, and America's Founders. This adaptation also is the theme of the essays in Paul Rahe, ed., *Machiavelli's Liberal Republican Legacy* (Cambridge, UK: Cambridge University Press, 2006), spanning English revolutionary republicanism, the moderate Enlightenment, and America's Founders.

8. For an overview of this argument see, Kissinger, *World Order*; Walter Russell Mead, *Special Providence: American Foreign Policy and How It Changed the World* (New York: Routledge, 2002); and Jonathan Monten, "The Roots of the Bush Doctrine: Power, Nationalism, and Democracy Promotion in U.S. Strategy," *International Security* 29, no. 4 (Spring 2005): 112–56.

9. John T. Scott and Robert Zaretsky, "Why Machiavelli Still Matters," *New York Times*, 9 December 2013, http://www.nytimes.com/2013/12/10/opinion/why-machiavelli-matters.html; John Danford, "Getting Our Bearings: Machiavelli and Hume," in *Machiavelli's Liberal Republican Legacy*, edited by Paul Rahe (Cambridge, UK: Cambridge University Press, 2006), 94–120, esp. 95; William Landon, *Politics, Patriotism and Language: Niccolò Machiavelli's "Secular Patria" and the Creation of an Italian National Identity* (New York: Peter Lang Publishing, 2005), 79.

10. Walter Russell Mead, "Stratblog: The Virtues of Machiavelli," *The American Interest*, 2 April 2011, http://www.the-american-interest.com/2011/04/02/stratblog-the-virtues-of-machiavelli/.

11. Reinhold Niebuhr, *The Irony of American History* (1952; repr., Chicago, IL: University of Chicago Press, 2008); and Paul Elie, "A Man for All Reasons," *The Atlantic*, November 2007, http://www.theatlantic.com/magazine/archive/2007/11/a-man-for-all-reasons/306337/.

12. Barack Obama, "Remarks by the President at the Acceptance of the Nobel Peace Prize" (press release, Office of the Press Secretary, Oslo, Norway, 10 December 2009), https://www.whitehouse.gov/the-press-office/remarks-president-acceptance-nobel-peace-prize.

13. Leslie Gelb, *Power Rules: How Common Sense Can Rescue American Foreign Policy* (New York: HarperCollins Publishers, 2009), ix.

14. Negotiations for the Trans-Pacific Partnership (TPP) finally concluded in October 2015 and will require President Obama to secure majority support from both houses of Congress, deep in the fourth quarter of his presidency, amid an election year and when his relations with Congress on both domestic and foreign policy are at their lowest point. While the TPP could be a victory for his pivot strategy on Asia, a high price paid for this multiyear effort is that China has secured territorial and military gains in the interim.

15. Roger Harrison, "Machiavelli Speaks: A Realist Raised from the Dead," *The American Interest*, 16 December 2014, http://www.the-american-interest.com/2014/12/16/a-realist-raised-from-the-dead/.

16. Walter Russell Mead, "Grand Strategy: The End of History Ends," *The American Interest*, 2 December 2013, http://www.the-american-interest.com/2013/12/02/2013-the-end-of-history-ends-2/; Victor Davis Hanson, "A New Obama Doctrine? *National Review*, 18 March 2014, http://www.nationalreview.com/article/373523/new-obama-doctrine-victor-davis-hanson; David Rothkopf, "Obama's 'Don't Do Stupid Shit' Foreign Policy," *Foreign Policy*, 4 June 2014, http://foreignpolicy.com/2014/06/04/obamas-dont-do-stupid-shit-foreign-policy/; and Stephen Walt, "What Putin Learned from Reagan," *Foreign Policy*, 17 February 2015, http://foreignpolicy.com/2015/02/17/what-putin-learned-from-reagan-ukraine-nicaragua/.

17. Analysts and journals usually sympathetic to the Obama presidency have issued stark appraisals of the international costs of the deal; one made just weeks after it survived Congressional review (with distinctly minority support) is David Rothkopf, "Leave It to Vlad (and the Supreme Leader): The Obama Plan to Exit the Middle East Now Becomes Clear," *Foreign Policy*, 28 September 2015.

18. Niccolò Machiavelli, *The Prince*, translated by Harvey Mansfield, 2nd ed. (1985; repr., Chicago, IL: University of Chicago Press, 1998), 100.

19. Ibid., chapter 23, 94.

20. See also, Bob Woodward, *Obama's Wars* (London, UK: Simon & Schuster UK Ltd., 2010); and Stanley McChrystal, *My Share of the Task* (New York: Penguin Group, 2013).

21. Machiavelli, *The Prince*, chapter 23, 93.

22. Carnes Lord, *The Modern Prince: What Leaders Need to Know Now* (New Haven, CT: Yale University Press, 2004); Gelb, *Power Rules*; and Ignatieff, "Machiavelli Was Right."

23. Friedrich Meinecke, *Machiavellism: The Doctrine of Raison D'Etat and Its Place in Modern History*, translated by Douglas Scott (1924; repr., New York: Praeger, 1965); Leo Strauss, *Thoughts on Machiavelli* (Chicago, IL: University of Chicago Press, 1958); and Harvey Mansfield, *Machiavelli's Virtue* (Chicago, IL: University of Chicago Press, 1996).

24. Mansfield, *Machiavelli's Virtue*, ix.

25. Machiavelli, *The Prince*, chapter 15, 61.

26. Maurizio Viroli, *Redeeming the Prince: The Meaning of Machiavelli's Masterpiece* (Princeton, NJ: Princeton University Press, 2014).

27. Machiavelli, *The Prince*, chapter 26, 101.

28. Viroli, *Redeeming the Prince*, 3.

29. In Shakespeare's Henry VIII, Act III, Sc. 1, Cardinal Wolsey utters this line when, undone by ambition to promote himself, he is exposed as serving the Pope (the Vatican corporation) instead of his country. George Carey and James McClellan, eds., *The Federalist, by Alexander Hamilton, John Jay, and James Madison, Gideon Edition* (Indianapolis, IN: Liberty Fund, 2001), 9.

30. See Jay's reference to the weak Italian republic of Genoa genuflecting before the King of France at the end of Federalist No. 3; see also Jay at the end of Federalist No. 4, wherein he warns, "What a poor, pitiful figure will America make in their eyes!"

31. Henry Kissinger, America's Machiavelli figure as national security advisor and secretary of state to US presidents during the Cold War, is an exception that proves the rule. His later works take into account moral sentiment of the American people as a source of US power, almost as a lesson learned from his younger years in government when idealism, at the time, seemed needlessly to constrain or derail effective (Machiavellian) foreign policy. Compare *Does America Need a Foreign Policy*, *On China*, and *World Order* to earlier works such as *Diplomacy* and *White House Years*. Henry Kissinger, *Does America Need a Foreign Policy* (New York: Simon and Schuster, 2001); *On China* (New York: Penguin Press, 2011); *World Order* (New York: Penguin Press, 2014); *Diplomacy* (New York: Simon and Schuster, 1994); and *White House Years* (Boston, MA: Little Brown & Co., 1979).

32. Samuel Huntington, "American Ideals versus American Institutions," *Political Science Quarterly* 97, no. 1 (Spring 1982): 1–37; and George Kennan, "Morality and Foreign Policy," *Foreign Affairs* (Winter 1985/86): 205–18.

33. Monten, "The Roots of the Bush Doctrine;" Nye, *Presidential Leadership and the Creation*; Stephen Sestanovich, *Maximalist: America in the World from Truman to Obama* (New York: Alfred A. Knopf, 2014); and Feaver, *Strategic Retrenchment*.

34. Machiavelli, *The Prince*, chapter 8, 37–38.

35. Markus Fischer, *Well-Ordered License: On the Unity of Machiavelli's Thought* (Lanham, MD: Lexington Books, 2000); and Markus Fischer, "Machiavelli's Rapacious Republicanism," in *Machiavelli's Liberal Republican Legacy*, edited by Paul Rahe (Cambridge, UK: Cambridge University Press, 2006), xxxi–lxii.

36. Strauss, *Thoughts on Machiavelli*, 67.

37. For these crucial lines, often cited as the essence of Machiavelli's strategic thought, we follow the model of literary analysis pioneered in W. Robert Connor's work on Thucydides' text, *History of the Peloponnesian War*. W. Robert Connor, *Thucydides* (Princeton, NJ: Princeton University Press, 1984). In this same vein and influential in the Brady–Johnson Grand Strategy Program at Yale is Charles Hill, *Grand Strategies: Literature, Statecraft and World Order* (New Haven, CT: Yale University Press, 2010).

38. Machiavelli, *The Prince*, chapter 18, 71.

39. Robert Gates, *Duty: Memoirs of a Secretary at War* (New York: Alfred A. Knopf, 2014); Leon Panetta, *Worthy Fights* (New York: Penguin Press, 2014); Jeffrey Golberg, "Hillary Clinton: 'Failure' to Help Syrian Rebels Led to the Rise of ISIS," *The Atlantic*, 10 August 2014, http://www.theatlantic.com/international/archive/2014/08/hillary-clinton-failure-to-help-syrian-rebels

-led-to-the-rise-of-isis/375832/; Juliet Eilperin, "Hillary Clinton Criticizes President Obama's Foreign Policy in Interview with the Atlantic," *Washington Post*, 11 August 2014, http://www.washingtonpost.com/politics/hillary-clinton-criticizes-president-obamas-foreign-policy-in-interview-with-the-atlantic/2014/08/11/46d30564-2170-11e4-8593-da634b334390_story.html; and Jeffrey Goldberg, "A Withering Critique of Obama's National Security Council" (interview with David Rothkopf, author of *National Insecurity* [New York: Public Affairs, 2014]) *The Atlantic*, 12 November 2014, http://www.theatlantic.com/international/archive/2014/11/a-withering-critique-of-president-obamas-national-security-council/382477/.

40. For measured analyses stating concerns and criticism about the JCPOA from experienced American diplomats and from public figures supportive of President Obama on other policies, see Henry Kissinger and George Shultz, "The Iran Deal and Its Consequences," *Wall Street Journal*, 7 April 2015 (addressing the initial Framework deal); Dennis Ross, "Iran Deal Leaves U.S. with Tough Questions," *Washington Post*, 14 July 2015, "How to Make Iran Keep Its Word," *Politico Magazine*, 29 July 2015; Walter Russell Mead, "The Strategic Impact of the Iran Deal," *The American Interest*, 5 August 2015; and Charles E. Schumer, "My Position on the Iran Deal," *Medium* (blog), 6 August 2015, https://medium.com/@SenSchumer/my-position-on-the-iran-deal-e976b2f13478.

41. Barack Obama, *National Security Strategy* (Washington, DC: White House, February 2015), https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf. For critical reviews, see Peter Feaver, "Grading Obama's National Security Strategy 2.0," *Foreign Policy*, 6 February 2015, http://foreignpolicy.com/2015/02/06/grading-obamas-national-security-strategy-2-0/; and Thomas Wright, "Interpreting the National Security Strategy," Up Front (blog), Brookings Institution, 6 February 2015, http://www.brookings.edu/blogs/up-front/posts/2015/02/06-interpreting-the-national-security-strategy.

42. Rothkopf, "Obama's 'Don't Do Stupid'."

43. Machiavelli, *The Prince*, chapter 18, 69.

44. "It is better to be impetuous than cautious." "Fortune is a woman . . . [and] like a woman, she is the friend of the young because they are less cautious, more ferocious, and command her with more audacity." Ibid., chapter 25, 101.

45. Realists insist there is moral value in effectiveness, and it is hard to be an effective great power by promising human rights protection or democratic transformation abroad then failing to deliver for lack of resources or resourcefulness. Sean Kay, *America's Search for Security: The Triumph of Idealism and the Return of Realism* (Lanham, MD: Rowman & Littlefield, 2014), 20. We grant this. Nonetheless, most moral choices, including in world politics, involve increased risks or costs not utter destruction in the line of duty. Realism as a prescriptive theory goes too far, becomes amoral, and loses sight of a deeper prudence when it teaches leaders of great states to sacrifice nothing, ever, for higher purposes. Kay provides examples of the situations in Iran in 1979, Rwanda in 1994, and Egypt in 2011. In contrast, see Paul Carrese, "The Grand Strategy of Washington and Eisenhower: Recovering the American Consensus," *Orbis* 59, no. 2 (Spring 2015): 269–86. Carrese challenges the reading of Dwight Eisenhower as narrowly realist and cautious.

46. This is the view of the response to Machiavelli developed by America's Founders, in the chapters on Washington (by Matthew Spalding) and Hamilton (by Karl Walling) in *Machiavelli's Liberal Republican Legacy*, edited by Paul Rahe (Cambridge, UK: Cambridge University Press, 2006).

47. Machiavelli, *The Prince*, chapter 21, 91.

48. Goldberg, "A Withering Critique."

49. Machiavelli, *The Prince*, chapter 18, 70.

50. For a critical but respectful analysis of the Florentine's contributions to modern strategic studies, see David Hendrickson, "Machiavelli and Machiavellism," in *Machiavelli's Legacy: The Prince After 500 Years*, edited by Timothy Fuller (Philadelphia, PA: University of Pennsylvania Press, 2016). Our broad conception of grand strategy draws upon philosophical approaches, such as Hill, *Grand Strategies*, and more policy-oriented views, as in Peter Feaver et al., *Strategic Retrenchment*, 3, and Peter Feaver, "What is Grand Strategy and Why Do We Need It?," *Foreign Policy*, 8 April 2009.

51. For more on enlightened self-interest and sources for this concept in American strategy, see Carrese, "The Grand Strategy of Washington and Eisenhower."

Deterrence Stability in the Cyber Age

Edward Geist

Abstract

Technical and operational realities make it prohibitively difficult to adapt a Cold War paradigm of "deterrence stability" to the new domain of cyber warfare. Information quality problems are likely to forestall the development of a cyber equivalent of the strategic exchange models that assessed deterrence stability during the Cold War. Since cyberspace is not firmly connected to geographic space the way other domains are, modeling is extremely difficult, muddling the neat conceptual distinctions between "counterforce" (military) and "countervalue" (civilian) targets. These obstacles seriously complicate US planning for a credible cyber "assured response" and present substantial challenges to potential adversaries contemplating cyber attacks against US interests. To create a maximally effective deterrent against cyber threats, the United States should seek to maximize the challenges for possible opponents by creating a cyber "strategy of technology," emphasizing resilience, denial, and offensive capabilities.

✳ ✳ ✳ ✳ ✳

On 19 March 2015, Adm Michael S. Rogers, head of US Cyber Command (USCYBERCOM), declared in testimony before the Senate Armed Services Committee that the United States needs to field offensive cyber capabilities. Complaining that the White House has not yet delegated authority to USCYBERCOM to deploy offensive tools, Rogers expressed his concern that "in the end, a purely defensive, reactive strategy will be both late to need and incredibly resource-intense," drawing the conclusion that "we need to think about: how do we increase our capacity on the offensive side to get to that point of deterrence?" The admiral's message found a ready audience among the committee members. Concurring that "I just think it's critical to develop an offen-

---

Edward Geist is a MacArthur Nuclear Security Fellow at the Center for International Security and Cooperation at Stanford University and former Stanton Nuclear Security Fellow at the RAND Corporation. He earned a PhD in history from the University of North Carolina and has published articles in the *Journal of Cold War Studies, Russian Review, Slavic Review*, and the *Bulletin of the History of Medicine*.

sive cyber-capability," Sen. Angus King (I-ME) went so far as to invoke Stanley Kubrick's classic 1964 film *Doctor Strangelove*. "If you build the doomsday machine, you've got to tell people you have it. Otherwise the purpose is thwarted."[1]

Should the "delicate balance of terror," as RAND strategist Albert Wohlstetter termed the Cold War nuclear standoff, be imported into the cyber domain? While the conceptual simplicity of "mutual assured destruction" seems intuitive, Wohlstetter's famous 1958 essay of that title offers a timeless warning to those who would presume that deterrence is either easy or straightforward. "Perhaps the first step in dispelling the nearly universal optimism about the stability of deterrence," he cautioned, "would be to recognize the difficulties in analyzing the uncertainties and interactions between our own wide range of choices and the moves open to the Soviets." Far from being a desirable end goal per se, in his view strategic deterrence was an unpalatable necessity. While deterrence constituted "a keystone of a defense policy," Wohlstetter implored, "it is only a part, not the whole," and he concluded that "we have talked too much of a strategic threat as a substitute for many things it cannot replace."[2]

In the wake of Wohlstetter's article, US defense analysts deployed a suite of increasingly sophisticated tools for gauging the delicate balance of terror. These models of how a nuclear exchange between the superpowers might play out in turn became a cornerstone of the field of deterrence stability. By fielding nuclear forces capable of mounting a devastating retaliation even in the aftermath of a well-planned preemptive strike, both the United States and the Soviet Union (USSR) would be deterred from risking nuclear war.

Can this Cold War paradigm of deterrence stability be adapted to the new domain of cyber warfare? However attractive this prospect might appear, technical and operational realities make it prohibitively difficult. In particular, information quality problems are likely to forestall the development of a cyber equivalent of the strategic exchange models that undergirded assessments of deterrence stability between the Cold War superpowers. The fact that cyberspace is not firmly connected to geographic space the way other domains are makes such models extremely difficult to construct and muddles neat conceptual distinctions between "counterforce" (military) and "countervalue" (civilian) targets. While these obstacles seriously complicate US planning for a credible cyber

"assured response," they also present substantial challenges to potential adversaries contemplating cyber attacks against US interests. Without the ability to model the effects of cyber attacks, proper US policies and capabilities would likely dissuade rational actors from mounting assaults that might fail to have the intended effect while eliciting a devastating retaliatory response from the United States. Therefore, to create a maximally effective deterrent against cyber threats, the United States should seek to maximize these challenges for possible opponents.

Accomplishing this goal will require a comprehensive cyber "strategy of technology," emphasizing the goals of resilience (minimizing the probable damage from a successful attack), denial (minimizing the probability an attack will succeed), and offensive capabilities. Such an approach—robust enough to confront the most sophisticated state-level adversaries—would also be more effective than a deterrence strategy against nonstate actors that might not be dissuaded by rational strategic calculations. While ideally this framework would cover both US government entities and civilian property, its high upfront cost would likely limit initial federal investment to systems critical for executing US military operations and protecting essential civilian infrastructure. However, private industry should be encouraged to employ similar techniques to increase resilience of its own assets. In contrast to the Cold War, when the nature of strategic nuclear weapons made "deterrence by denial" an impossible dream, in cyberspace the United States can present potential adversaries with a highly obfuscated and constantly evolving attack surface, dissuading adversaries by undermining their faith in prospects of success.

Operations Research and the Cyber Domain

"Operations analysis" first emerged as a distinct field during the Second World War in response to new technologies that posed the same kind of unprecedented concerns for the military as emerging cyber capabilities do today. According to RAND analyst E. S. Quade, "the major impetus for this activity was provided by the introduction of new weapons systems based on, and requiring for their operation, technical know-how foreign to past military experience." Originally directed largely at tactical questions such as how to best employ or disrupt novel technologies such as radar, in the postwar years operations analysis evolved into "systems analysis" as researchers began to evaluate longer-term weapons

development projects with much higher degrees of uncertainty. During the 1950s weapons system analysts, particularly at the RAND Corporation, began expanding their purview to investigate sweeping questions of strategy and national defense policy.[3]

Nuclear weapons presented merely the most novel hurdle to defense analysts during the early Cold War. They confronted a furiously evolving technological landscape in which entire new fields, such as digital computing, quickly transitioned from laboratory experiments to critical components of military hardware. The initial temptation to dismiss the technical competence of communist adversaries, furthermore, swiftly proved naïve. Confident predictions that the USSR would require at least a decade, if not more, to field its own nuclear weapon were dashed by the first Soviet atomic test in 1949. In 1953 the USSR tested a rudimentary deliverable thermonuclear weapon, arguably beating the United States on this front by several months. Aggressive Soviet pursuit of ballistic missile technology paid off spectacularly a few years later, when the USSR used the R-7 intercontinental ballistic missile (ICBM) to launch Sputnik in October 1957. While Soviet propagandists crowed that their artificial moon proved the regime was making good on the Bolshevik promise to "bring fairy tales to life," many Americans panicked in response to a widespread perception that the United States was losing its technical edge—and possibly the Cold War along with it.[4]

Defense analysts at RAND and elsewhere weaponized America's intellectual potential to counter the communist threat. They deployed—or, in many cases, conceived—the latest mathematical and technological innovations to make the problems of superpower conflict tractable. In addition to adapting tools originally conceived for economics and industrial management to questions of war and defense, systems analysts applied novel methods such as Monte Carlo simulations, linear programming, and primitive digital computers to "think about the unthinkable," as futurist Herman Kahn termed it.[5]

These intellectual currents coalesced into a new art known as "modeling" or "model-building," which in turn has served ever since as a foundation—often implicit—for much of strategic thought. Concepts such as *assured destruction* hinged on the assumption that one could model the course of a nuclear exchange accurately enough to predict that a sufficiently large retaliatory force would, in fact, survive a well-planned preemptive strike. Figures from across the strategic spectrum deployed

models to justify their particular answer to the ever-controversial question of "how much is enough?" In time, an entire discipline of "deterrence stability" grew up around analyses of this type.

The concept of *deterrence stability* emerged out of the debate during the late 1950s and early 1960s about the merits of "mutual" or "minimal" deterrence. In contrast to the Eisenhower administration's declared policy of "Massive Retaliation," which held that the United States needed to maintain absolute strategic superiority over the USSR to make its deterrent threats credible, the proponents of mutual or minimal deterrence argued that a finite force would dissuade Soviet aggression so long as it was survivable. While eschewing demands for an arms buildup on the scale of the 1950s, the minimal deterrence framework did not provide a clear answer to just how large such a retaliatory force needed to be to deter the Kremlin effectively. In 1960 Daniel Ellsberg at RAND wrote an influential piece titled "The Crude Analysis of Strategic Choices" that offered an explicit formalization of Wohlstetter's concept of deterrence. By estimating the "payoffs" for US and Soviet "strike first" and "strike second" strategies, Ellsberg's model aimed to help elucidate which policy choices would discourage the USSR from attempting a first strike. "The precise effects of a change in military 'posture,' policy, or plans upon these [utility estimates] are, of course, hard to determine, uncertain, and subject to controversy," he noted, but "nevertheless, rough estimates are often made, and these are, in fact, the basis for most policy recommendations as to choices among military alternatives."[6]

Ellsberg's model provided the foundation for the analysis of strategic postures in terms of deterrence stability, and the tantalizing prospect of identifying what would be sufficient to deter the Kremlin soon found approval among policy makers. In 1971, Pres. Richard Nixon declared that "our policy remains . . . to maintain strategic sufficiency," which he defined as "the maintenance of forces adequate to prevent us and our allies from being coerced." Furthermore, "stability . . . also means numbers, characteristics, and deployments of our forces which the Soviet Union cannot reasonably interpret as being intended to threaten a disarming attack."[7] However, estimating just what it would take to achieve these goals proved to be fraught with difficulty, and in the 1970s and 1980s an immense amount of ink was spilled about how deterrence stability should be analyzed, modeled, and estimated. Despite widespread consensus about the overall assumptions of the deterrence stability frame-

work, which could encompass a spectrum of strategic philosophies from minimal deterrence to war fighting, vociferous debate ensued about how to model the superpower nuclear balance and determine how many weapons would deter Soviet coercion without appearing threatening.[8]

Attempts to gauge the nuclear balance of terror between the superpowers employed a wide array of methodologies, but the assumed characteristics of nuclear weapons and delivery systems provided some common points of reference. In particular, nearly all of the models analyzed the problems of delivery system performance and target survivability in spatial terms. Furthermore, reconnaissance satellite photos and other intelligence data made it possible to estimate the number and probable characteristics of enemy bombers and missiles. While vociferous debates erupted between defense analysts in the United States over questions such as the exact yields of Soviet ICBM warheads and their accuracy, uncertainties for these values were well within an order of magnitude, and many of them made little impact on model outputs anyhow. From the metric of "equivalent megatonnage," which linearized the total destructiveness of superpower nuclear arsenals on the basis of the total area their warheads could theoretically expose to a certain blast overpressure, to the more sophisticated "counterforce potential" that incorporated accuracy to estimate an arsenal's total ability to hold hardened targets such as ICBM silos at risk, to full strategic exchange models that aimed to estimate how many weapons would be available to retaliate after a preemptive strike, analysts generally assumed that nuclear war could be reduced to measures of radii and area.

This commonality aside, models of strategic nuclear forces assumed a dazzling array of forms, but one in particular, the "sufficiency model," played an outsized role in public discussions of deterrence stability. As John A. Battilega and Judith K. Grange wrote in 1978, "strategic nuclear forces have given birth to a special class of models used to roughly assess the absolute and relative sufficiency of the U.S. strategic nuclear force posture, and, conversely, to assess the significance of foreign nuclear force postures." Typically falling "into the category of static or quasi-dynamic measures of effectiveness," the "primary use" of such models was "to provide a vehicle for the discussion of such concepts as strategic parity, deterrence, and stability." According to the authors, "the role of such models has evolved uniquely in connection with nuclear forces." Factors including "the definition of U.S. strategic deterrence objectives

in ways which required relative comparisons with foreign adversaries, . . . the requirement to popularly debate, but in a semi-technical language, the major U.S. nuclear weapons programs, . . . [and] the requirement to think through major U.S. deterrence, strategy, and force-sizing options in a way which could be understood but which did not refer to historical experience with nuclear warfare" drove this evolution. Troublingly, this ubiquity sometimes led to these models being employed for purposes for which they were not necessarily suited: "these models are sometimes used as primary or secondary measures of effectiveness in force planning or force interaction," the authors noted, "but it should be remembered that the reason for this use stems from their historical evolution as sufficiency models."[9]

Useful as the concepts of deterrence stability and strategic sufficiency were in the policy debates of the late Cold War, by the 1990s their limitations became more and more apparent. Increasingly elaborate derivatives of Ellsberg's initial framework exacerbated a shortcoming Ellsberg admitted in 1961: the need to assign values to variables without any real-world justification for doing so.[10] Furthermore, deterrence stability and strategic sufficiency proved difficult to translate into the multipolar post–Cold War geopolitical landscape. In South Asia, the emergence of India and Pakistan as new nuclear powers offers a particularly pressing real-world countercase to elegant mathematical models of strategic stability. Unlike the Cold War superpowers, which both feared a preemptive nuclear strike, New Delhi and Islamabad both envision that nuclear use would grow out of an all-too-conceivable conventional confrontation along the countries' contested border. The additional presence of China, a long-established nuclear power, further complicates the regional strategic picture. The multiplicity of actors, along with the diversity of possible scenarios, makes it extremely challenging to model deterrence stability in this part of the world.[11] The limitations of such modeling approaches in the nuclear domain suggest that we should hesitate before importing them into emerging arenas, such as cyber warfare.

Modeling Cyber: Wrong but Useful

For better or for worse, we cannot construct sufficiency models to estimate deterrence stability in the cyber domain precisely because cyberspace differs so much from the conventional domains. Cyberspace is not measured in inches and miles, nor can the effectiveness of cyber

weapons be reduced to a simple measure of destructive radius. Neither cyber weapons nor their potential targets have the sort of predictable evolution that nuclear weapons did during the Cold War. Qualitatively, new weapons such as ICBMs only appeared after years of warning and usually took at least a few years beyond that to become truly operational. Furthermore, although delivery systems became more accurate and hardened targets grew marginally more survivable, the effects of nuclear weapons remained constant, even if scientific understanding of them continued a fitful evolution. By contrast, a radical new cyber weapon with never-before-seen effects could appear overnight, or a timely patch or upgrade might render a well-designed cyber attack impotent. The disconnect between cyberspace and physical space also makes it difficult to distinguish between counterforce and countervalue targets or to restrict collateral damage. As the Stuxnet case dramatically demonstrated, it can be difficult to construct a powerful cyber weapon without running the risk it will affect systems other than its intended targets. In light of such uncertainties, it is very hard indeed to imagine a cyber equivalent to the Cold War models that estimated the superpowers' relative nuclear might.

This is not to say that comprehensive models of cyberwar are impossible to build. Such models can and should be created, but the qualitative characteristics of cyberspace and the uncertainties involved render them unable to provide the kind of confident predictions essential to make assessments of strategic stability. As the eminent British statistician George E. P. Box famously put it, "essentially, all models are wrong, but some are useful."[12] What are the challenges of modeling cyber conflict, and to what purposes can such models reasonably be put?

Unfortunately, models of cyber war require a vastly higher level of sophistication than Cold War nuclear strategic models to be useful. Most models of nuclear conflict, such as the Arsenal Exchange Model, estimate the effects of attack on the basis of intersecting probability distributions in a two- or three-dimensional space.[13] Using the circular coverage function, estimates of delivery vehicle accuracy and target hardness can readily produce a probability estimate that the target will be destroyed. This calculation could be carried out using a slide rule, and in the early years of the Cold War, it usually was. Models used for estimating strategic stability generally neglected the temporal element altogether. By contrast, the effects of cyber attacks can only be modeled through the use

of dependency graphs. Computers and networks are targeted for cyber attack specifically because they are (or are perceived to be) connected to some type of resource or activity that the attacker hopes to interrupt, manipulate, or disrupt. Mathematically, such systems can be treated as directed graphs with edges representing the influence of different parts of the network upon each other. Since these influences can only travel forward in time, the system should be treated as a directed acyclic graph in which each node in the network is represented by a different node in the graph for each moment in the system's evolution. Furthermore, each of these nodes is likely to react differently depending on its internal state. Clearly, this is not the sort of problem one can readily solve with a slide rule![14]

Thankfully, there exists a variety of computational approaches that can be applied to create models of system response to cyber attacks. So long as the system is not too large, it should be possible to use object-oriented programming to simulate the dependency graphs explicitly. In fact, the first object-oriented programming language, Simula, was invented in the 1960s for simulation purposes. An object-oriented cyber-attack model could be as finely detailed as its builders cared to make it and as extensive as available computing resources would allow. This could facilitate the use of such models to investigate possible interactions between cyber, kinetic, and nuclear attacks. Despite these attractions, an object-oriented approach is liable to require tremendous amounts of analyst manpower to construct, and it is not the only possible way to model cyber war. Finite element analysis, for instance, might be adapted to model certain kinds of cyber attacks.[15]

In addition to their relative complexity, models of cyber war are likely to be extremely sensitive to the information used to construct them. The structure of the dependency graph and the reaction of its nodes to particular stimuli depending on their state are likely to result in huge qualitative differences in the output results. In contrast to a nuclear attack, where one would hardly expect a single nuclear burst to destroy dozens of discrete targets simultaneously, in the cyber domain a well-placed attack on a vulnerable node might cause the prompt failure of all its dependencies. However, both the dependencies of any particular node—as well as its vulnerabilities—may be extremely difficult to ascertain in advance. Without good-quality intelligence about both of these factors, models of cyber attack cannot have predictive value.

What purpose, then, can such models serve? The above qualities make cyber models potentially useful for operations planning for theater campaigns but of dubious utility for creating broader political-military policy strategies. In the operational realm, models of cyber attack could be useful for research purposes even when constructed on a purely notional basis. For instance, such models could be created specifically to explore the possible dynamics of multidomain operations combining cyber with nuclear or kinetic operations. By offering a concrete framework in which to investigate various hypotheses about how such interactions could play out, these simulations could provide invaluable insights—even if they could not predict the success of any particular operation. These lessons could then be applied to reduce the cyber vulnerabilities of the United States and its strategic partners. With the benefit of sufficient information about target systems, such models could also be employed for operational planning, although the considerable amount of effort needed to construct the model and the potentially limited shelf life of the reconnaissance data are apt to make this extremely challenging.

However, for strategic assessment, models of cyber attack are dubious at best and liable to be downright harmful. The analytic categories that made models useful for studying nuclear deterrence stability translate poorly into the cyber domain. If there is a cyber analog of assured destruction, policy makers can never count on it due to the immense uncertainties that would be attendant on the construction of a cyber strategic model. Furthermore, the data collection necessary to implement such a model would itself be fraught with peril, as it would require making a comprehensive assessment of all US cyber vulnerabilities. Should such an assessment, or even a fraction of it, fall into the hands of an adversary, the damage to US security would be astronomical.

The Implausibility and Undesirability of Cyber Assured Destruction

The intrinsic uncertainties of planning cyber offensives have not dissuaded some observers from insisting that in cyberspace, the timeworn maxim "the best defense is a good offense" applies more than ever. "Although the United States must demonstrate that it has in its toolkit the requisite items for use against hostile parties when necessary, there has not been a clear cut public demonstration of cyber dominance to

date of which the US has definitively taken and actively sought ownership," complained Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi in a 2012 article. "Against this background, should the United States consider engaging in the digital equivalent of an aboveground nuclear test?" This drastic measure, the authors asserted, "is not to be dismissed out of hand, . . . [as] if conducted with care (commensurate to the enormity of the exercise) [it] may be instrumental to deterring hostile actors."[16]

The widespread inclination to conceptualize cybersecurity problems in a framework analogous to that developed to characterize the superpowers' nuclear stalemate is all the more unaccountable given that Cold War nuclear strategists hardly considered apocalyptic possibilities as something to be welcomed. US and Soviet scientists alike expended herculean efforts attempting to craft viable defenses against nuclear attack, only to stumble in face of insurmountable technical obstacles. Deterrence constituted an unpalatable necessity that American and Soviet leaders found themselves compelled to embrace.

Does cyber attack share the characteristics that made deterrence the least-negative option in the nuclear domain? Some official assessments have asserted as much. In 2012 the Defense Science Board (DSB) concluded "the cyber threat is serious, with potential consequences similar in some ways to the nuclear threat of the Cold War." Characterizing an "existential cyber attack" as "capable of causing sufficient wide-scale damage for the government potentially to lose control of the country," the DSB asserted that this might be accomplished by adversaries who "can invest large amounts of money (billions) and time (years) to actually create vulnerabilities in systems, including systems that are otherwise strongly protected." While thankfully such "capabilities are today limited to just a few countries such as the United States, China, and Russia," the DSB asserted that "since it will be impossible to fully defend our systems against [such] threats, deterrence must be an element of an overall risk reduction strategy."[17]

However, accounts no less authoritative have discounted the probability of existential cyber attacks. Director of National Intelligence James R. Clapper reported to the Senate Armed Services Committee on 26 February 2015 that while "cyber threats to US national and economic security are increasing in frequency, scale, sophistication, and severity of impact . . . the likelihood of a catastrophic attack from any particular

actor is remote at this time." In Clapper's assessment, "Rather than a 'Cyber Armageddon' scenario that debilitates the entire US infrastructure, we envision something different." Instead of a digital apocalypse engineered by Russia or China, Clapper foresaw "an ongoing series of low-to-moderate level cyber attacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security."[18] With no Armageddon in prospect, does it really make sense to seek a cyber assured-destruction capability?

In any case, the would-be instigators of an existential cyber attack would find themselves stymied by the modeling challenges thus outlined. A cyber assault capable of causing the government to lose control over part of the country would almost certainly require mounting sophisticated attacks against multiple systems simultaneously, quite possibly in coordination with kinetic actions against critical targets. However, given the difficulty of assembling reliable intelligence essential to plan such an attack, much less model its likely dynamics, how would an adversary have sufficient confidence of its chances of success? Thus, only an extremely desperate or foolhardy opponent would be likely to take such a course of action—precisely the kind of less-than-rational actor who might not be deterred in any case. It is therefore hardly surprising that Paul K. Davis, one of the United States' most-experienced model builders, opined in a RAND working paper that "deterrence by itself is a fragile basis for strategic thinking." In his view, "hoping for deterrence with today's reality would be like grasping for straws. Deterrent measures should definitely be part of strategy, but the focus should be elsewhere."[19]

A Cyber Strategy of Technology

If deterrence based upon assured destruction cannot serve as the centerpiece of US cyber strategy, what can? Fortunately, the same fundamental challenges that complicate our efforts to model the effectiveness of offensive cyber operations also bedevil our probable opponents. With foresight, the United States can craft a strategy that aims to forestall cyber attack by exacerbating these difficulties as much as possible for would-be attackers. Through a combination of increasing the resilience of US systems and undertaking measures intended to obstruct and confuse enemy intelligence-gathering efforts, the United States can dissuade

both state and nonstate adversaries from attempting the most audacious cyber attacks by denying them confidence in their likely success.

In 1970 Stefan T. Possony and J. E. Pournelle expressed the concern that the USSR, unlike the United States, pursued a "technological strategy" that might deliver them victory in the superpower rivalry without firing a shot. Despite Soviet economic and technical inferiority, the ability to focus a greater share of its more limited resources on military research and development, as well as simply steal technologies from the West when convenient, might allow the Kremlin to field superior forces—particularly if the United States allowed itself to become complacent. Defining "technological warfare" as "the direct and purposeful application of the national technological base and of specific advances generated by that base to attain strategic and tactical objectives," Possony and Pournelle declared that "genuine Technological War aims at reducing the use of firepower in all forms to a minimum."[20] Emphasizing that "like all wars, the Technological War requires a deliberate strategy," they suggested that the aim of such a strategy ought to be "to make the enemy counter each move that you make, and to dance to your tune."[21]

The United States should adopt such a "strategy of technology" to address the cyber threats of the twenty-first century. This strategy should comprise three basic strands. The first of these, *resilience*, aims to protect critical US infrastructure by increasing its ability to withstand enemy action. The second, *dissuasion by denial*, aims to complicate planning for attacks on US cyber assets by increasing the difficulty of intelligence collection and analysis for potential adversaries. The third component consists of a comprehensive *offensive cyber capability*—not as a standalone deterrent; however, because if opponents take steps similar to those outlined above, this deterrent will have serious credibility problems. Instead, the offensive cyber capability will serve two purposes. First, the United States must possess a firm grasp of the "state of the art" in offensive cyber techniques so as to identify essential measures for the resilience and denial missions. Second, the offensive capability needs to complement US defense planning for conventional, space, and nuclear operations.

To improve the resilience of its own and civilian cyber systems, the Department of Defense (DOD) should partner with private industry in a long-term effort to reduce the vulnerabilities exploited by cyber attacks. While eliminating all vulnerabilities is an unattainable goal, US security would benefit from potential adversaries possessing a less

plentiful choice of attack vectors. There is good reason to believe that the barriers to secure software and hardware are primarily institutional and cultural in origin rather than technical. Many older codebases were developed in an era when present-day security challenges were totally inconceivable, and traditional software engineering practices deemphasized security concerns in favor of controlling costs and meeting deadlines. While the DOD began funding research into methods to prove the correctness of programs starting in the 1960s, these made almost no impact on the way either the US defense sector or private industry developed their systems, in part because such research took many decades to bear fruit. Researchers initially hoped to develop techniques that could be applied to software written in existing programming languages, only to find that proving the correctness of even the most trivial program in a language such as FORTRAN was forbiddingly difficult. Provably correct programs, it turned out, would require a paradigmatically different approach to programming and hardware engineering. Academic researchers began developing such techniques in the 1970s, but these remained impractical for many decades as both theory and implementation slowly improved. Furthermore, there was little demand for secure systems and software until relatively recently. While the DOD sought them out for certain applications, the private sector saw little need to pay the extra expense for features that appeared totally superfluous. With a captive defense market and the ubiquitous cost-control problems, there was little incentive to either produce secure systems and software at an affordable price point or to develop the human capital and technology needed for doing so. Fortunately, there is good reason to believe that there is a way to surmount these obstacles.

Recognizing that present-day approaches will not be adequate to meet the future needs of the US military, in 2012 the Defense Advanced Research Projects Agency (DARPA) embarked on a program to pioneer the creation of secure combinations of hardware and software on the basis of formal methods such as theorem-proving. Dubbed "High-Assurance Cyber-Military Systems," this project aims "to create technology for the construction of high-assurance cyber-physical systems, where high assurance is defined to mean functionally correct and satisfying appropriate safety and security properties."[22] As a demonstration, the DARPA developed a remote-controlled drone quadcopter so secure that its "red

team" of hackers could not discover any vulnerabilities in it even after the opportunity to study the complete source code for a period of six weeks.[23] This feat suggests that secure software and hardware are not just a pipe dream, but it requires a development process very alien to usual practices. Widespread adoption of such technology, even just for defense purposes, will require the establishment of a whole new culture of system development, including training large numbers of programmers and engineers in radically different ways of thinking. This transition would be difficult and expensive, but it may prove the only way to protect US assets from increasingly sophisticated cyber attacks.

Private industry is also devoting increasing attention to the possibility of employing formal methods to limit its cyber vulnerabilities. Facing increasingly steep liabilities from cyber attacks against commercial interests, in recent years the technology industry has invested ever-greater resources in qualitatively improved software engineering techniques that greatly reduce the incidence of such vulnerabilities. For instance, the Mozilla Foundation has been aggressively developing Rust, a systems programming language that aims to liberate coders from the manual memory management that so often introduces serious security holes into software.[24] Another promising approach is the use of functional programming languages such as Haskell, which aim to enable the creation of nontrivial programs with provably correct behavior by forcing software to be written in accordance with strict mathematical formalisms. While radically different from the imperative programming style familiar to most programmers, this type of functional programming has attracted growing attention from security researchers because it promises to enable the creation of software with a radically reduced number of security vulnerabilities.[25] Although the Department of Homeland Security has ongoing programs to encourage more secure software engineering practices, the DOD—thanks to its extensive purchasing power—can help accelerate the development and adoption of these technologies and the replacement of vulnerability-ridden legacy code.[26]

Although more challenging to alleviate, hardware vulnerabilities often result from similar legacy issues and engineering oversights. US civilian cyber infrastructure grew organically out of technologies that were originally engineered prior to the emergence of the kind of security threats that are all too common today. Decades later, this heritage provides adversaries with a wide array of hardware exploits to compromise US sys-

tems. A transition to fundamentally more secure technologies would be both lengthy and highly disruptive, possibly requiring a fundamental reconceptualization of the internet's technical underpinnings but might in the long term prove necessary to protect US interests. As a consequence, the DOD should subsidize efforts to develop qualitatively more secure network hardware for its own use and encourage similar efforts by the private sector with the goal of protecting civilian systems that support military operations, and ultimately, the United States as a whole.

To deny potential adversaries easy access to critical systems, the United States can shroud accurate knowledge about known or suspected vulnerabilities in a fog of disinformation and noise. Although not practical in all cases, there is little reason why systems of particular concern, such as military command and control and civilian power grids, could not create a vast number of decoys that ape their signature in cyberspace. If particularly well-engineered, these systems will appear similar enough to the real thing to fool would-be cyber attackers that they have penetrated their target—while feeding these adversaries carefully prepared disinformation intended to either deceive them about real vulnerabilities or to encourage them to commit mistakes revealing their identity and intentions.[27] Confronted by a large number of such decoys, hackers would be hard-pressed to discern reality from willful falsehood, greatly increasing the difficulty of conducting the technical reconnaissance that makes complex cyberattacks possible. The United States can make this strategy even more effective by undertaking technical measures increasing the rate at which the "real" attack surface changes. While attempting to obscure all systems in this fashion would be far too expensive and crowd out legitimate network traffic, the defense community might be able to forge a productive partnership with private industry to craft the requisite technology base, as that sector also has select assets to protect.

Finally, given the increasing use of information technology by potential adversaries, the United States should develop offensive cyber capabilities to complement military operations in other domains and to identify and ameliorate US vulnerabilities. In a future conflict, the ability to compromise enemy assets by exploiting cyber vulnerabilities could make victory less costly in terms of both blood and treasure. Furthermore, without a state-of-the-art cyber offensive capability comparable to that possessed by potential adversaries, red teaming against our own systems will be of unacceptably low quality. However, while the

United States should cultivate offensive cyber capabilities, it would be a mistake to develop these around the goal of deterrence, given that the qualitative nature of the cyber domain poses forbidding obstacles to escalation control. Without reliable models to assess the relative strength of different states' offensive cyber capabilities, or estimate the effects of cyber attacks, the concept of deterrence stability makes little sense in cyberspace. SSQ

Notes

1. Ellen Nakashima, "Cyber Chief: Efforts to Deter Attacks against the U.S. Are Not Working," *Washington Post*, 19 March 2015, http://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html.

2. Albert Wohlstetter, *The Delicate Balance of Terror* (Santa Monica, CA: RAND, 1958), http://www.rand.org/about/history/wohlstetter/P1472/P1472.html.

3. E. S. Quade, "Introduction," in *Systems Analysis and Policy Planning: Applications in Defense* (New York: Elsevier, 1968), 2–3.

4. For an account of the "missile gap" panic that followed Sputnik, see Peter J. Roman, *Eisenhower and the Missile Gap* (Ithaca, NY: Cornell University Press, 1995).

5. On the early institutional history of RAND, see Bruce L. R. Smith, *The RAND Corporation: Case Study of a Nonprofit Advisory Corporation* (Cambridge, MA: Harvard University Press, 1966). On the study of nuclear war at RAND in the early Cold War, see Fred Kaplan, *The Wizards of Armageddon* (Stanford, CA: Stanford University Press, 1983).

6. Daniel Ellsberg, *The Crude Analysis of Strategic Choices* (Santa Monica, CA: RAND, 1960). A condensed version of Ellsberg's RAND report appeared as "The Crude Analysis of Strategy Choices," *American Economic Review* 51, no. 2 (May 1961): 472–78.

7. Richard M. Nixon, *Public Papers of the Presidents of the United States, Richard Nixon: Containing the Public Messages, Speeches, and Statements of the President 1971* (Washington, DC: Government Printing Office, 1972), 310.

8. Although both advocates of arms limitation employed Ellsberg's framework to advance their arguments, attacks on its underlying assumptions emerged by the early 1970s. For instance, see Douglas E. Hunter, "Some Aspects of a Decision-Making Model in Nuclear Deterrence Theory," *Journal of Peace Research* 9, no. 3 (1972): 209–22.

9. John A. Battilega and Judith K. Grange, eds., *The Military Applications of Modeling* (Wright-Patterson AFB, OH: Air Force Institute of Technology Press, 1981), 245–46.

10. One important example of such an elaboration is Glenn Kent and David Thaler's first-strike stability model. Glenn A. Kent and David A. Thaler, *First-Strike Stability: A Methodology for Evaluating Strategic Forces* (Santa Monica, CA: RAND, 1989). For a critique of the Kent/Thaler model, see Stephen J. Cimbala and James Scouras, *A New Nuclear Century: Strategic Stability and Arms Control* (Westport, CT: Praeger, 2002), 1–23.

11. For a recent assessment of this subject, see the essays in Michael Krepon and Julia Thompson, eds., *Deterrence Stability and Escalation Control in South Asia* (Washington, DC: Stimson Center, 2013).

12. G. E. P. Box and N. R. Draper, *Empirical Model-Building and Response Surfaces* (New York: John Wiley and Sons, 1987), 424.

13. Battilega and Grange, *Military Applications of Modeling*, 283–89.

14. Ibid., 381–400. Models with these characteristics were developed during the Cold War to assess the survivability of US command, control, and communications (C3) systems. Historical examples included the Minimum Essential Emergency Communications Network

(MEECN) and STRAT Command, used by the USAF to evaluate C3 links to the strategic bomber force.

15. Finite element analysis is widely employed in engineering for analyzing complex problems. It works by subdividing a complex system of partial differential equations (PDE) into smaller subdomains that can be approximated by a simpler subset of the PDEs. Certain applications of finite element analysis in science and engineering suggest that it may be efficacious for modeling certain types of cyber attacks. For instance, the use of the technique to model the spread of infectious disease could be analogous to the spread of malware across a network of heterogeneous systems. See for instance Joshua P. Keller, Luca Gerardo-Giorda, and Alessandro Veneziani, "Numerical Simulation of a Susceptible–Exposed–Infectious Space-Continuous Model for the Spread of Rabies in Raccoons across a Realistic Landscape," *Journal of Biological Dynamics* 7, Supplement 1 (2013): 31–46.

16. Frank J. Cilluffo, Sharon L. Cardash, and George C. Salmoiraghi, "A Blueprint for Cyber Deterrence: Building Stability through Strength," *Military and Strategic Affairs* 4, no. 3 (December 2012): 15–16.

17. Department of Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, 2013), 2, 6.

18. James R. Clapper, director of national intelligence, "Statement for the Record Worldwide Threat Assessment of the US Intelligence Community Senate Armed Services Committee," 26 February 2015, http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf.

19. Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyberwar" (working paper WR-1049, RAND, June 2014), 1.

20. Stefan T. Possony and J. E. Pournelle, *The Strategy of Technology: Winning the Decisive War* (Cambridge, MA: Dunellen, 1970), 4, 8.

21. Ibid., 5, 15.

22. John Launchbury, "High-Assurance Cyber Military Systems (HACMS)," Defense Advanced Research Projects Agency (DARPA), no date, http://www.darpa.mil/program/high-assurance-cyber-military-systems.

23. Kathleen Fisher, "Using Formal Methods to Enable More Secure Vehicles: DARPA's HACMS Program" (presentation, Tufts University, 16 September 2014), http://wp.doc.ic.ac.uk/riapav/wp-content/uploads/sites/28/2014/05/HACMS-Fisher.pdf.

24. Mozilla Foundation, "The Rust Programming Language," no date, http://www.rust-lang.org/.

25. For instance, see David Terei, Simon Marlow, Simon Peyton Jones, and David Mazières, "Safe Haskell," *Proceedings of the 5th Symposium on Haskell*, September 2012, 137–48.

26. Department of Homeland Security (DHS), "Build Security In," no date, https://buildsecurityin.us-cert.gov/. DHS also operates the Continuous Diagnostics and Mitigation program, which aims to provide "federal departments and agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first." See DHS, "Continuous Diagnostics and Mitigation," 14 September 2015, http://www.dhs.gov/cdm.

27. "Social engineering"—manipulating individuals to divulge sensitive information—is a critical part of many cyber attacks, but disinformation could mislead adversaries into compromising themselves.

A Homeland Security Net Assessment Needed Now!

Erik J. Dahl

Abstract

The concept of net assessment has long been considered an important tool for American national security strategists, and the Pentagon's Office of Net Assessment is widely regarded as a key influence in security planning. However, despite calls by experts for the development of a similar net assessment office in the Department of Homeland Security (DHS), only a few tentative efforts have been made to use the concepts and methodologies of net assessment for the problem of ensuring American homeland security. This article argues that a homeland security net assessment is even more necessary today, since debates over the state of the nation's security involve discussions not only about the seriousness of the threat but also the legitimacy of the intelligence and other efforts employed to combat that threat. It proposes a new model for a homeland security net assessment process that should be undertaken by DHS and suggests that such an assessment would expand the discussion of homeland security threats beyond terrorism and would encourage greater focus on civil liberties and disaster preparedness.

✳ ✳ ✳ ✳ ✳

The concept of net assessment has long been considered an important tool for American national-security strategists, but this tool is largely unavailable in the effort to analyze threats and strategies in the areas of homeland security and homeland defense. The Pentagon's Office of Net Assessment (ONA) is famous within the American national-security

---

Erik Dahl is an associate professor of national security affairs at the Naval Postgraduate School and serves on the faculty of the Center for Homeland Defense and Security. He is the author of *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Georgetown University Press, 2013). A retired Naval intelligence officer, Dahl received his PhD from the Fletcher School of Tufts University and holds master's degrees from the Fletcher School, the Naval War College, and the London School of Economics.

establishment for its influence in security planning, but many critical homeland security threats are outside its scope. Additionally, there is no equivalent net assessment office within the DHS. Despite calls by experts for the development of such a capability within the DHS, only a few tentative efforts have been made to use the concepts and methodologies of net assessment for ensuring US homeland security. A comprehensive homeland security net assessment must involve more than a detailed understanding of external threats. Traditionally, national-security net assessments focus on two key factors: the enemy and one's own forces. To develop a homeland security net assessment, it is more critical to understand our own actions and capabilities, because those actions are focused within America's borders. In the areas of homeland security and defense, more than in traditional national security, governmental actions are likely to have a direct effect on the American people and society. For this reason, a homeland security net assessment must focus not only on the threat but also on our own capabilities to counter that threat.

Debates over the state of the nation's security involve discussions not only about the seriousness of threats from terrorism and other sources but also consideration of the legitimacy of the intelligence and other counterterrorism capabilities being employed to combat those threats. Of particular interest is the effect domestic intelligence programs have on civil liberties and domestic society. Other studies have examined the potential organizational structure of a DHS office of net assessment, so that is not the focus here.[1] Instead, the article proposes a framework for thinking about the task of a homeland security net assessment and suggests a new model for the process that should be undertaken by the DHS in assessing the key threats to the US homeland, which are terrorism, cyber, and natural hazards like disasters and infectious disease. It begins by reviewing the concept of net assessment and how it has been used in the US Department of Defense (DOD). Next it examines proposals for the DHS to establish an office of net assessment following the DOD model and then posits how the process of net assessment should be modified for the problem of homeland security, using a new model that could be adopted by the DHS. The final section offers preliminary suggestions and implications from such a homeland security net assessment process.

What Is Net Assessment?

The concept of net assessment arose during the Cold War, when the United States realized that traditional tools and systems for analyzing national-security challenges did not include any place or procedure for carefully integrating assessments of the enemy threat with an understanding of one's own capabilities. Intelligence agencies and officials typically refrained from analyzing "blue force" capabilities, while operational planners, who did understand US capabilities, could not be sure they were privy to the best (and often most-highly classified) intelligence information on the enemy against whom they were planning. Additionally, there was no institutional advocate for taking a long-term, strategic-level approach to national-security problems; within the intelligence community and the policy establishment, current problems and issues invariably prevented senior analysts and decision makers from being able to think about long-term goals and threats.

Net assessment is closely identified with Andrew Marshall, the founder and, until recently, director of the DOD's ONA.[2] Marshall and his office became famous among strategic thinkers, and several think tanks and analysts have adopted the net-assessment idea. A few scholars have suggested that net assessments should become more widely used today, but the concept remains relatively little known outside defense circles.[3]

Early in his tenure, Marshall wrote that national assessments "are intended to provide insight for policymakers at the highest levels by discovering and illuminating the nature of major national security problems."[4] The key element of a net assessment is a comparison of two sides in interaction with one another. In the words of Eliot Cohen, "Net assessment is the appraisal of military balances."[5] It might strike an observer as self-evident that strategists and military planners should be taking into account assessments of both sides of a situation. After all, Sun Tzu famously advised that a general must "know the enemy and know yourself; in a hundred battles you will never be in peril."[6] But in fact, this is only rarely done. As the authors of a Carnegie Endowment net assessment put it, "only a net assessment requires the analyst to have an understanding of the capabilities of friendly forces. Although obtaining an understanding of friendly forces sounds easy—especially for government analysts—it can be anything but."[7]

Although the net-assessment approach has been used most notably by the Pentagon, it does not focus only on military factors. The DOD

defines net assessment as "the comparative analysis of military, technological, political, economic, and other factors governing the relative military capability of nations. Its purpose is to identify problems and opportunities that deserve the attention of senior defense officials."[8] Most advocates of net assessment see it as a broad-based, interdisciplinary approach, taking into account not only military matters but also economic, political, technological, and social factors.

Net assessments involve both quantitative and qualitative analysis. Even in assessments of the military balance between two countries, which might lend themselves to a largely quantitative analysis, advocates prefer to avoid a strictly numbers-based approach. Cohen, for example, argued during the Cold War that it was important "to get beyond mere 'bean counting'" and understand how each side operated its forces. The focus is on the long term, identifying long-term trends and looking beyond the typical US government perspective that is often shaped by the length of a presidential administration.[9] As Aaron Friedberg notes, "Trends are important because the past will always shape, even if it does not completely determine, the future."[10] Paul Bracken writes, "One of the greatest contributions of net assessment is that it calls for consciously thinking about the time span of the competition you are in."[11] In fact, this long-term view may be one reason why the Pentagon's ONA has been seen as successful. It can be hard to criticize assessments about a future that is decades away.

Another key aspect of the Pentagon's net-assessment approach—and another likely reason why it has been supported through so many administrations—is that it does not produce specific policy recommendations. As one critic has put it, "It could be the case that Marshall's approach has survived precisely because it is so oracular and nebulous."[12] Marshall himself writes that net assessment should "aim at providing diagnosis of problems and opportunities, rather than recommended actions. The focus on diagnosis rather than solutions is especially significant."[13] He explained in an interview that the need to provide policy prescriptions can "corrupt the analysis," because it will tend to blur objectivity. He said, "People psychologically favor certain policies and then distort the analysis. In order to get [an] even handed, objective approach you [need] to . . . constrain it to the diagnosis problem."[14]

It is often said that the Pentagon's ONA has encouraged pessimistic thinking and worst-case scenarios. During the late years of the Cold

War, for example, Cohen argued that a net-assessment approach helped to demonstrate the weakness in the analysis of some authors and scholars who he called optimists, who believed that the conventional military balance in Europe at the time favored the North Atlantic Treaty Organization rather than the Warsaw Pact.[15] More recently, one critic has called the ONA "a full-time office of threat inflation,"[16] and some have charged that Marshall and the ONA tend to exaggerate threats—in particular concerning China, which has been the subject of a great deal of ONA-sponsored work in recent years. Marshall acknowledged in an interview that "We tend to look at not very happy futures."[17]

Recently the occasion of Marshall's retirement and the publication of a highly favorable book about him by two former colleagues have generated a small flurry of articles assessing his legacy. Supporters, such as Andrew Krepinevich and Barry Watts, laud him as "an intellectual giant comparable to such nuclear strategists as Bernard Brodie, Herman Kahn, Henry Kissinger, James Schlesinger, and Albert Wohlstetter."[18] He has been praised for being one of the first to understand the importance of what became known as the "revolution in military affairs" and for warning about the rise of China long before the current administration's pivot to Asia.[19] Critics, on the other hand, argue he was far from all-knowing—having missed the increasing threat of terrorism prior to the 9/11 attacks. Critics also contend that, because most of the products of the ONA are classified, it is difficult to objectively assess the value of its work.[20]

The debate over Andrew Marshall's legacy will undoubtedly continue.[21] However, the continuing value of the net-assessment approach seems clear, especially in areas of homeland security and defense, where it is especially important to match our understanding of external threats with a clear-eyed assessment of our own internal capabilities.

The DHS and Net Assessment

There is no central office or organization in the US government responsible for producing net assessments focusing on homeland security issues. The National Counterterrorism Center (NCTC) is chartered with having the primary responsibility within the US government for conducting net assessments of terrorist threats.[22] However, its work appears to be mostly classified. Therefore, it is not known whether it con-

ducts regular net assessments, and if it does, whether those assessments are useful to policy makers. Some elements of the DHS, such as the Domestic Nuclear Detection Office (DNDO), do appear to conduct net assessments. That office has as one of its functions the mission of performing red team and net assessments.[23] However, many observers have argued that the DHS should make greater use of net assessments and should establish a net assessment office similar to the Pentagon's ONA.

In 2007, for example, the Homeland Security Advisory Council issued a report calling on the DHS to "establish an Office of Net Assessment (ONA) within the Department to provide the Secretary with comprehensive analysis of future threats and U.S. capabilities to meet those threats."[24] That same year a report by the Heritage Foundation argued that the DHS should form a small, nonpartisan office of net assessment that would be able to focus on long-term challenges and help address the complaint by the 9/11 Commission and others that the nation suffered from a "lack of imagination."[25] A strong advocate of establishing a net-assessment capability within the DHS has been Frank J. Cilluffo, the associate vice president and director of the Center for Cyber and Homeland Security at The George Washington University. Cilluffo argues that the DHS responds to most threats reactively and has only a limited capability for assessing future threats:

> The ONA would fill the much-needed role of brain trust, while remaining unfettered by the "crisis du jour" or the day-to-day demands flowing from intelligence needs and operations. The ever-shifting and unpredictable security environment facing the United States requires the constant questioning of assumptions, the asking of what-ifs, and the thinking of the unthinkable, all in order to identify game changers. The ONA should take a comprehensive, multi-disciplinary approach to its analysis, looking at the full range of factors which will alter and shape the security environment of the future, including social, political, technological, economic, demographic, and other trends.[26]

One particular area in which a net assessment has been called for is bioterrorism. In 2004 the Bush administration published Homeland Security Presidential Directive 10, *Biodefense for the 21st Century*, which called for "a periodic senior-level policy net assessment that evaluates progress in implementing this policy, identifies continuing gaps or vulnerabilities in our biodefense posture, and makes recommendations for re-balancing and refining investments among the pillars of overall defense policy."[27] Such a net assessment was reportedly conducted, but it has not been publicly released.[28]

Patrick Forrest and Alex Hilliker argue that because homeland threats and challenges such as public safety, emergency management, and law enforcement are largely outside the scope of the DOD, the existing ONA in the Pentagon is insufficient to deal with such important matters. Instead, they argue, a new office of net assessment is needed within the DHS to provide long-term strategic assessments of future security threats—without being subject to the many reporting requirements that are placed on existing DHS offices such as the Office of Strategic Plans. They write that DHS leadership has suffered from a lack of data-driven, long-term threat assessments, and as a result billions of dollars have been spent on ineffective programs such as the Secure Border Initiative Network. Furthermore, they suggest that a relatively small, independent office reporting directly to the Secretary of Homeland Security be established, the focus of which "would be solely on producing assessments intended to increase the leadership's situational awareness regarding future challenges to the homeland security enterprise."[29]

A New Net-Assessment Model for Homeland Security

In recent years national-security leaders have frequently argued that the threats facing America's security today are more challenging than those seen in the past. Testifying before the Senate, Director of National Intelligence James Clapper stated, "Looking back over my now more than half a century in intelligence, I've not experienced a time when we've been beset by more crises and threats around the globe."[30] Gen Martin Dempsey, the chairman of the Joint Chiefs of Staff, testified, "I will personally attest to the fact that it [the world] is more dangerous than it has ever been."[31] Some critics have charged that such dire warnings are exaggerations, and Secretary of Homeland Security Jeh Johnson has not taken quite such a pessimistic view.[32] However, Johnson has also made it clear that the threat is serious: "The United States faces a constantly evolving threat environment. Thirteen years after the 9/11 attacks, threats to our nation have not subsided."[33]

What threats should be part of a homeland security net assessment? Clearly, one focus would be on the terrorist threat to the United States. Secretary Johnson has said, "The cornerstone of our mission at the Department of Homeland Security has been, and should continue to be, counterterrorism—that is, protecting the nation against terrorist at-

tacks."[34] A focus on terrorism suggests that a homeland security net assessment should compare the threat from specific groups or actors, such as al-Qaeda or the Islamic State in Iraq and the Levant (ISIL), with the counterterrorism capabilities available to combat them. Although estimates of the terrorist threat are available in abundance, there appear to be few, if any, net assessments available that would compare the terrorist threat with US counterterrorism capabilities.[35]

Even though terrorism might be considered "job one" for homeland security, it is neither the only threat nor the only mission for the homeland security enterprise.[36] *The 2014 Quadrennial Homeland Security Review* found that terrorism is only one of several primary homeland security concerns: "The terrorist threat is increasingly decentralized and may be harder to detect. Cyber threats are growing and pose ever-greater concern to our critical infrastructure systems as they become increasingly interdependent. Natural hazards are becoming more costly to address, with increasingly variable consequences due in part to drivers such as climate change and interdependent and aging infrastructure."[37] These three categories of challenges—terrorism, cyber, and natural hazards—may provide a useful and more complete framework for understanding the threats that would be examined by a homeland security net assessment.

Few observers would be surprised by the inclusion of terrorism and cyber threats on this list, but some, especially those within the DOD, might wonder why natural hazards should be considered a key homeland security problem. After all, the mission of providing military support to civil authorities following a natural disaster or other emergency is typically considered a secondary one for military planners. However, for homeland security planners and practitioners, disasters and other types of natural hazards are a primary mission—and a mission that has been growing in recent years, following disasters such as Hurricane Katrina, super storm Sandy, and occurrences of other natural threats such as the outbreak of infectious disease. The Obama administration has acknowledged the link between natural hazards and national security. In the 2015 *National Security Strategy* the White House noted that ensuring national security means "reinforcing our homeland security to keep the American people safe from terrorist attacks and natural hazards while strengthening our national resilience."[38]

However, there is more to a net assessment than an examination of the threat. It must also provide decision makers with an understanding of our own capabilities, and this aspect is even more important in the area of homeland security than national security. Political scientist Rose McDermott has noted that the second part of Sun Tzu's advice—the need to know oneself—is especially important in the field of homeland security: "Certainly for purposes of homeland security, recognizing our own gaps and failings is an important part of triumphing over our limitations."[39] The adversary may not be far away in a distant land but instead can be here in the middle of the homeland. The capabilities developed to counter homeland security threats will tend to involve and affect a broader range of American citizens than will the military, foreign policy, and intelligence capabilities that are used to counter foreign threats.

A homeland security net assessment, then, might examine the threats from terrorism, cyber, and natural hazards and the capabilities that have been developed to address each of these threats. But that, too, would not be enough. Because homeland security efforts are directly focused within US borders, they must also consider the effect of those efforts on the American people and society. If a national-security net assessment is the appraisal of military balances, as Cohen described it, then a homeland security net assessment should be the appraisal of other, equally important balances, such as the balance between security and liberty that is at the forefront of many discussions of homeland security. The requirement to understand the effects of our policies on the American people might be captured in the concept of *legitimacy*: are the capabilities our government has developed to keep us safe seen as legitimate in the eyes of the people they are designed to serve?

There is nothing new in arguing that domestic and public concerns are critical for understanding threats and strategies. Advocates of net assessment often cite Clausewitz approvingly, noting his argument that war is an extension of politics by other means—implying that both political and military issues must be involved in conducting a true net assessment.[40] Even more appropriate for our purposes may be what Clausewitz referred to as the "remarkable trinity." This trinity has often been translated as the people, the army, and the government; Clausewitz argued that war is the product of the interaction of these three forces, and a strategist can only understand war by understanding all three.[41]

A similar homeland security trinity may be helpful in understanding the forces that must be understood to conduct a homeland security net assessment. This trinity involves the *threats*, *capabilities*, and *legitimacy* involved in homeland security.[42] Thus, our proposed homeland security net assessment process would examine the threat to America's security in three broad categories: terrorism, cyber, and natural hazards. And for each threat, the assessment would examine the nature of that threat, the capabilities to counter the threat, and whether those capabilities are seen by the American people as legitimate or are seen as risking civil liberties or other democratic values. The next section will undertake to sketch out what such a homeland security net assessment might reveal.

A Preliminary Homeland Security Net Assessment

Although the Pentagon's ONA has often been seen as a source of pessimistic, worst-case thinking, a homeland security net assessment would be most useful for policy makers if it were seen as producing objective, fact-based reports on long-range trends and issues concerning the most important threats facing the nation. These assessments could fill a niche in between the pessimistic studies often produced by outside critics of whichever administration is in power and the considerably more optimistic reports typically issued from government agencies when they attempt to assess their own accomplishments. The following are some of the issues and problems a homeland security net assessment could help illuminate.

Terrorism

America's current domestic intelligence structure encompasses a complex system that includes counterterrorism organizations led by the NCTC; other federal-level organizations and efforts, including those within the Federal Bureau of Investigation (FBI), the DHS, and the DOD; and state, local, and private-sector activities. Despite the development of these counterterrorism organizations and capabilities, many experts argue much more remains to be done, especially in terms of coordinating federal efforts with those of state, local, and private entities. A recent report by a panel of experienced practitioners and scholars argues that, "The United States still lacks a cohesive domestic counterterrorism strategy with the capacity for coordinated execution at all levels of government."[43] Even though

the threat from al-Qaeda has declined, the overall terrorist threat today remains high, with a broad range of groups and individuals continuing to pose significant threats to American lives at home and abroad. Some experts believe the terrorist threat is greater today than it was in the immediate post-9/11 period, but the growing consensus is that while the threat of another catastrophic attack appears reduced, there remains a continuing threat of smaller-scale plots and attacks from al-Qaeda affiliates and homegrown extremists.[44]

In its analysis of the terrorist threat facing the United States, a homeland security net assessment would need to take a broad, long-range view. It must also consider the impact of more recent events such as the death of Osama bin Laden, the upheaval of the Arab Spring, and the rise of ISIL.[45] The last *National Intelligence Estimate* written (or at least made public) on the terrorist threat to the United States was in 2007, suggesting that a new assessment is overdue. Such an assessment might reflect the conventional view among terrorism experts that al-Qaeda has been weakened in recent years, largely as a result of the counterterrorism efforts that have been undertaken by the United States and its allies since 2001. A recent report by the Bipartisan Policy Center describes some of these improved capabilities:

> For example, on 9/11, there were 16 people on the U.S. "no fly" list. Today, there are more than 40,000. In 2001, there were 32 Joint Terrorism Task Force "fusion centers," where multiple law enforcement agencies work together to chase down leads and build terrorism cases. Now there are 103. A decade ago, the U.S. Department of Homeland Security, National Counterterrorism Center, Transportation Security Administration, Northern Command, and Cyber Command didn't exist. In 2014, all of these new post-9/11 institutions make it much harder for terrorists to operate in the United States.[46]

An assessment will also need to consider the rising threat from lone-wolf terrorists and other homegrown extremists. It could examine the quantitative data that is available on such threats. As Secretary Johnson has said, "This is the type of threat that may be hardest to detect. It involves independent actors potentially living in the United States, with easy access to items that, in the wrong hands, can become tools for mass violence."[47] The New America Foundation, for example, has found that homegrown jihadist extremists have killed 26 people since 9/11, while non-jihadist extremists have killed 39.[48] However, the assessment would also have to wrestle with more difficult questions about how to measure and compare different kinds of threats facing the nation. For example,

during the same week in which the Boston Marathon bombings killed three people, a fertilizer plant exploded in West, Texas, killing 14. The Boston bombings received much more media attention, but a net assessment might consider whether the risks from industrial accidents or other kinds of disasters represent a greater homeland security threat than terrorism. An example of such a perspective can be found in the work of Brian Jenkins, who has noted that the level of terrorist violence in the United States during the past decade has been considerably less than that experienced during the 1970s, "when there were 50 to 60 terrorist bombings a year in the United States."[49] That statistic is likely to come as a surprise to most Americans, and one task for a net assessment would be to determine how significant such historical comparisons are for today.

One of the most important developments has been the establishment of a network of 78 state and local intelligence fusion centers, which typically receive DHS funding and support but are under local control. These fusion centers are not widely known, but they have had some notable successes in helping to prevent terrorist attacks and assisting law enforcement agencies in capturing criminals.[50] They have also generated controversy. A Senate committee report found that fusion centers "often produced irrelevant, useless or inappropriate intelligence reporting to DHS, and many produced no intelligence reporting whatsoever."[51] A RAND study examined fusion centers and the FBI-led Joint Terrorism Task Forces and reported, "What we found was organized chaos: a federally subsidized, loosely coordinated system for sharing information that is collected according to varying local standards with insufficient quality control, accountability, or oversight."[52] However, other experts and studies have argued that state and local fusion centers are a vital part of the homeland security enterprise, and a net assessment would be useful in asking questions such as, is 78 the right number of these centers?[53]

Some of the most important changes in counterterrorism capabilities have been improvements in domestic intelligence at the federal, state, and local levels. As Brian Jenkins notes, homeland security intelligence is likely to become even more important in the coming years: "Domestic intelligence collection is essential, especially as al Qaeda places more emphasis on inspiring local volunteers to take action."[54] Additionally, the intelligence gathered to detect such threats will almost inevitably need to sweep up information on American citizens who are not, themselves, threats. Gregory Treverton writes, "Today, it's not enough to

know about them; intelligence can't understand them without knowing a lot about 'us.'"[55] A homeland security net assessment might argue that in evaluating domestic intelligence programs, we should follow the same standard as the US Food and Drug Administration in determining whether drugs can be marketed: they need to be both safe and effective. This would mean that for counterterrorism intelligence programs to be judged legitimate and worthwhile, a program needs to be both effective in preventing terrorist attacks and sufficiently safe for civil liberties and personal freedoms.

Some of the most controversial American counterterrorism capabilities—such as the National Security Agency's (NSA) bulk data-collection programs that were revealed by Edward Snowden—may not pass this test. Not only is the legitimacy of these programs in question but also there is considerable debate over whether they are effective in preventing terrorism. Intelligence community leaders have claimed these programs are necessary for national security, but two official studies, by the President's Review Group and the Privacy and Civil Liberties Oversight Board, argued that at least one program—the collection of American phone data—had not been useful. Outside researchers have also found that bulk collection of phone data has not prevented a single terrorist attack.[56] The most effective domestic counterterrorism tools have been traditional law enforcement techniques such as the use of undercover officers and informants and close engagement with the local community to encourage tips from the public and from family members of those who might be at risk of radicalization.[57]

Finally, a net assessment would closely examine the legitimacy of American counterterrorism capabilities. One of the most important—and most controversial—of these capabilities is the use of unmanned drone strikes. Many critics of American policy view these strikes—often resulting in civilian casualties, including recently two hostages held by al-Qaeda—as illegitimate.[58] The rules governing drone use are not well understood by the public, and as the Bipartisan Policy Center writes, "The choices the United States makes regarding its use of drones for targeting killing operations and the rules that regulate such operations will shape the global environment in the coming decades."[59]

Cyber

Estimates of the threat from cyberterrorism range from the extremely dire to the moderately sanguine. Some scholars and computer-security experts argue that the nation faces the threat of a "cyber Pearl Harbor,"[60] while others claim threats of cyberwar are little more than a myth.[61] Former Secretary of Homeland Security Janet Napolitano warned that a "cyber 9/11" could happen "imminently."[62] On the other hand, a classified national intelligence assessment in 2013 concluded that cyberespionage, most notably from China, represented a greater threat to the nation's security than cyberterrorism.[63] And in his latest testimony to Congress, Director Clapper said the likelihood of a catastrophic "Cyber Armageddon" is remote.[64]

A net assessment could be especially useful in helping to advance the debate over the different kinds of cyber threats facing the nation. The Bipartisan Policy Center recently argued that a different approach is needed: "Overall, the cybersecurity debate has matured but does not yet sufficiently distinguish among the various threats. The next step must be a more nuanced approach to address this problem and a more careful use of terms—especially 'cyber attack,' 'cyber war,' and 'cyberterrorism.'"[65]

A net assessment, taking a long-term view and making use of available data on specific cyber threats, would likely conclude, as Colin Gray has written, "Despite the acute shortage of careful strategic thought on the subject, and notwithstanding the 'Cybergeddon' catastrophe scenarios that sell media products, it is clear enough today that the sky is not falling because of cyber peril."[66] It seems likely that a net assessment would adopt the relatively cautious approach taken by terrorism expert Martha Crenshaw, who notes that the most disruptive cyber attacks, such as the Stuxnet virus used against Iranian centrifuges, have been the work of sophisticated state actors—not terrorist groups or individuals.[67]

Just as the debate over the cyber threat is relatively new and underdeveloped, the discussion of cyber capabilities is also at a fairly undeveloped stage. The US military has established a Cyber Command (USCYBERCOM), as a four-star subunified command under the US Strategic Command, with the mission of directing DOD cyber operations and defending military information networks. The commander of USCYBERCOM also serves as director of the NSA, an intelligence organization that provides support to military and national customers, including USCYBERCOM.[68] Some critics worry the United States may

be combining too much military and civilian authority into one organization. Peter Singer of the Brookings Institution said, "The mashing together of the NSA and Cyber Command has blurred the lines between a military command and a national spy agency."[69] Other critics argue more needs to be done, such as creating a US Cyber Force that would operate alongside the existing military services.[70] Richard Clarke, who has been an outspoken advocate for concern about cyber threats, argues the United States needs to urgently develop greater cyber-defense capabilities: "If anything is clear, it is that we have a remarkably well-developed offensive capability, but no commensurately serious commitment to defense. There is neither a plan nor any capability to defend America's civilian infrastructure, from banking to telecoms to aviation."[71]

In recent years it seems as if just about everybody in the national security and intelligence communities has jumped on the cyber bandwagon, with other new cyber organizations including the Cyber Threat Intelligence Integration Center under the director of national intelligence, a new cyber directorate at the Central Intelligence Agency, and the National Cybersecurity and Communications Integration Center under the DHS. However, it is not clear if we have determined the proper "lanes in the road" for these different organizations. The history of the DHS suggests that once major organizational reforms have been made in government, it can be difficult to change course. The DHS often ranks low on surveys of federal government-employee satisfaction and is often criticized for being too big to manage effectively. Although it has undergone several reorganizations since it was first established, it is still largely as it was originally designed. The force of path dependence is strong in government organizations, and a homeland security net assessment would help us realize that the cybersecurity organizations we are establishing today are likely to be around for many years. It is important to think carefully from the beginning about how to deconflict responsibilities and avoid creating stovepipes.

Because cyber issues directly affect virtually all Americans, it is particularly important that a broad net assessment perspective, acknowledging the concerns of stakeholders beyond the traditional national security establishment, inform cyber strategies. The Pentagon understands that the problem of cybersecurity cannot be addressed by military personnel alone and is planning to create a "surge force" of

private-sector and National Guard cyber experts who could be called upon to help protect critical infrastructure sectors in case of a national cyber emergency.[72] Eric Rosenbach, the assistant secretary of defense for homeland defense and global security, has said the DOD is committed to a whole-of-government approach to cybersecurity, including close coordination with other federal agencies, state and local governments, and the private sector.[73] As Adm Michael Rogers, commander of USCYBERCOM and director of NSA, puts it, "Neither the U.S. government, the states, nor the private sector can defend their information systems on their own against the most powerful cyber forces. The public and private sectors need one another's help."[74]

A net assessment of America's cybersecurity would likely conclude that more work needs to be done to gauge the effect of increased cyber capabilities on civil liberties. As a National Research Council report noted, effective programs to deter viruses and other malware from Internet traffic may require the traffic to be inspected by a third party, which raises important privacy issues.[75] Additionally, from a homeland security perspective, one of the weaker areas of public policy may be at the level of state and local authorities. It appears the most significant cyber capabilities exist either at the level of the federal government, where most policies originate, or in the private sector, where most research and development is conducted. Some significant state and local efforts are underway, but more must be done, and a homeland security net assessment could help suggest areas of focus below the federal level.[76]

Natural Hazards

The disasters of Hurricane Katrina and super storm Sandy ensured that threats from natural hazards remain near the top of the list of homeland security concerns facing the nation. According to the *Quadrennial Homeland Security Review*, "Natural disasters, pandemics, and the trends associated with climate change continue to present a major area of homeland security risk."[77] The greatest natural-hazard risk, the review argues, is of a devastating pandemic, and the 2014 Ebola outbreak in West Africa provides support for that view.[78] However, the threat remains high from other kinds of natural disasters, including hurricanes, earthquakes, droughts, and floods, with the DHS noting the increasing risk as the nation's infrastructure ages and as climate change may act as a "threat multiplier."[79]

A homeland security net assessment would weigh such threats against the capabilities that have been developed to prepare for and respond to them. The DHS argues that the nation's capability to respond to natural hazards and disasters has improved significantly since Katrina: "Acting on the lessons of Hurricane Katrina, we have improved disaster planning with federal, state, local, tribal, and territorial governments, as well as nongovernmental organizations and the private sector; pre-positioned a greater number of resources; and strengthened the Nation's ability to respond to disasters in a quick and robust fashion. Seven years after Katrina, the return on these investments showed in the strong, coordinated response to Hurricane Sandy."[80]

The US government has developed a sophisticated national preparedness system, including a *National Preparedness Goal* that sets out 31 core national capabilities and a *National Preparedness Report* that summarizes the progress made in achieving those core capabilities.[81] Most experts agree the nation is better prepared for disasters than it has been in the past.[82] However, an area where more work needs to be done, and where a net assessment could be particularly useful, is in determining how effective these preparedness capabilities really are. The Government Accountability Office found that, "DHS and FEMA [Federal Emergency Management Agency] have implemented a number of efforts with the goal of measuring preparedness by assessing capabilities and addressing related challenges, but success has been limited."[83]

A number of scholars and homeland security practitioners have warned in recent years about the danger of what Paul Stockton, former assistant secretary of defense for homeland defense and Americas' security affairs, calls "catastrophes more severe than Hurricane Katrina."[84] Such disasters are sometimes called complex catastrophes, "black swans," or "wicked problems," and they appear to be increasing in frequency and seriousness.[85] An example that is often cited of such a potential catastrophe is an earthquake along the New Madrid fault, near the town of New Madrid, Missouri. An estimated magnitude 7.7 earthquake struck that region in 1812, killing few people in what was then an underpopulated area but causing tremendous shocks that collapsed the banks of the Mississippi River and liquefied the ground. Experts estimate that 86,000 people could be killed if a similar earthquake hits that area today.[86] FEMA conducted a National Level Exercise in 2011 focused on

the New Madrid threat, and a homeland security net assessment would be able to examine this type of high-impact but low-probability event.

Although it might not seem obvious that legitimacy is an important factor in ensuring homeland security against natural hazards, public acceptance of and support for government efforts may be more important in this area than any other. This is because local, public, and private-sector involvement is critically important in preparing for and responding to natural hazards and disasters. The DHS Strategic Plan argues that a "whole community approach" is necessary "to build the capacity of American society to be resilient in the face of disruptions, disasters, and other crises."[87] A homeland security net assessment would evaluate how successful the DHS has been in engaging the American public and other stakeholders in the effort to prepare for natural hazards and catastrophes.

Conclusion

This very preliminary review suggests that in the area of terrorism, there is currently a favorable—but tenuous—balance of threat and homeland security capabilities that has, thus far, succeeded in keeping America safer than most experts would have predicted after the 9/11 attacks. America's global counterterrorism efforts and domestic law enforcement and intelligence systems appear to have been successful in increasing security within the United States, as demonstrated by numerous foiled terrorist plots and the lack of another major successful attack on American soil since 9/11.

However, these gains have come at the cost of increasing domestic surveillance and at the risk of infringing upon civil liberties. By its very nature, domestic and homeland security intelligence is intrusive and risks impinging on civil liberties. As then-Secretary of Homeland Security Michael Chertoff put it, "Intelligence, as you know, is not only about spies and satellites. Intelligence is about the thousands and thousands of routine, everyday observations and activities. Surveillances, interactions—each of which may be taken in isolation as not a particularly meaningful piece of information, but when fused together, gives us a sense of the patterns and the flow that really is at the core of what intelligence analysis is really about."[88]

These thousands of observations are largely about people and events in America and, in the years since 9/11, the United States has created a

domestic intelligence system to collect them. In some cases the people are terrorists or other types of criminals, and the intelligence collected has helped to prevent bad events from happening. However, in many cases these observations—this domestic intelligence—is about routine activities undertaken by ordinary Americans and others who do not intend to cause harm.[89] A net assessment would examine whether these intelligence and counterterrorism capabilities are "safe and effective" and whether they are sufficiently legitimate or if they should be reexamined.

A net assessment would also be valuable in expanding the discussion of homeland security threats beyond terrorism. Looking at the balance among threat, capability, and legitimacy suggests more attention must be devoted to the impact of increased cyber capabilities on civil liberties and on the need for greater cyber-defense capabilities at the state and local levels. It also might highlight the need to develop better tools for measuring the nation's preparedness efforts to deal with natural disasters and with the potentially greater threat of complex catastrophes. Additionally, whenever possible, the products of such net assessments should be made unclassified and widely available. This is the right thing to do, because Americans deserve to know as much as can reasonably be shared about the actions their government is taking. It is also the strategic thing to do, because homeland security efforts are most effective when they are supported and trusted by the people they serve.

A final important step would be to look farther into the future, as net-assessment analysts in the Pentagon did during the Cold War. Paul Bracken notes that thinkers using the concept of net assessment were able to identify the importance of Asia as an area of strategic concern and competition as early as the 1980s, despite the fact that the only immediate problem of Asian security at that time was Korea.[90] The comparable question for today might revolve around what the rising threats and concerns for homeland security are not simply for the next few years but also for the next several decades.

In recent years we have seen a few, mostly tentative calls for the use of net assessment tools in determining and weighing the threats to America's homeland security. However, as we continue to face an increasing variety of challenges in an era of decreasing budgets and government retrenchment, these tools may be more useful than ever. As a first step, the DHS should establish an office of net assessment and direct it to

conduct a broad-based study of the threats from terrorism, cyber, and natural hazards. SSQ

Notes

1. For example, Patrick Forrest and Alex Hilliker, "Why the Department of Homeland Security Needs an Office of Net Assessment," *Risk, Hazards & Crisis in Public Policy* 3, no. 3 (September 2012): 1–18.

2. Mie Augier, "Thinking about War and Peace: Andrew Marshall and the Early Development of the Intellectual Foundations for Net Assessment," *Comparative Strategy* 32, no. 1 (January–March 2013): 1–17. For useful background on the history of the Office of Net Assessment (ONA) see Thomas M. Skypek, "Evaluating Military Balances through the Lens of Net Assessment: History and Application," *Journal of Military and Strategic Studies* 12, no. 2 (Winter 2010): 1–25, and Phillip A. Karber, "Net Assessment and Strategy Development for the Secretary of Defense: Future Implications from Early Formulations" (faculty paper, Georgetown University Institute of International Law and Politics, 15 August 2008), https://georgetown.box.com/s/9s11fgxsokczslxuccq5. Marshall retired in January 2015. Not surprisingly, given his low public profile, the event attracted little fanfare. For a succinct examination of his impact on Washington see "The Quiet American," *Economist*, 10 January 2015, http://www.economist.com/news/united-states/21638157-enigmatic-futurist-last-calls-it-quits-quiet-american.

3. Examples of recently produced net assessments include Peter Chalk, Angel Rabasa, William Rosenau, and Leanne Piggott, *The Evolving Terrorist Threat to Southeast Asia: A Net Assessment* (Santa Monica, CA: RAND, 2009); Mark Fitzpatrick, ed., *North Korean Security Challenges: A Net Assessment* (London: International Institute for Strategic Studies, July 2011); Michael D. Swaine, et al., *China's Military & the U.S.-Japan Alliance in 2030: A Strategic Net Assessment* (Carnegie Endowment for International Peace, 2013); and Michael D. Swaine, Mike M. Mochizuki, Michael L. Brown, Paul S. Giarra, Douglas H. Paal, Rachel Esplin Odell, Raymond Lu, Oliver Palmer, and Xu Ren, *Conflict and Cooperation in the Asia-Pacific Region: A Strategic Net Assessment* (Washington, DC: Carnegie Endowment for International Peace, 2015). For a discussion of a revival in interest in net assessment today, see Yee-Kuang Heng, "The Return of Net Assessment," *Survival* 49 no. 4 (Winter 2007–2008): 135–52.

4. Andrew W. Marshall, "National Net Assessment," memorandum for the record, 10 April 1973, 2. Available from the Digital National Security Archive, file no. 01198.

5. Eliot A. Cohen, *Net Assessment: An American Approach*, Jaffee Center for Strategic Studies Memorandum no. 29 (Tel Aviv: Jaffee Center for Strategic Studies, April 1990), 4.

6. Sun Tzu, "The Art of War," in *Strategic Studies: A Reader,* edited by Thomas G. Mahnken and Joseph A. Maiolo (New York: Routledge, 2008), 64.

7. Swaine, et al., *China's Military & the U.S.-Japan Alliance in 2030*, 8.

8. Department of Defense Directive 5111.11, *Director of Net Assessment*, 23 December 2009, 1.

9. Cohen, *Net Assessment*, 14–15.

10. Aaron L. Friedberg, "The Assessment of Military Power: A Review Essay," *International Security* 12, no. 3 (Winter 1987–1988), 193.

11. Paul Bracken, "Net Assessment: A Practical Guide," *Parameters* 36, no. 1 (Spring 2006), 94.

12. Michael C. Desch, "Don't Worship at the Altar of Andrew Marshall," *National Interest*, January–February 2015, http://nationalinterest.org/feature/the-church-st-andy-11867.

13. Marshall, "National Net Assessment," 1. It is worth noting that while Marshall prefers not to recommend policy options, he does believe it important for the net-assessment process to provide decision makers with *opportunities*. The difference between opportunities and policies may be a fine one, but it appears to have been enough to be useful to Marshall in defusing bureaucratic opposition toward his office.

14. Augier, "Thinking about War and Peace," 12.

15. Eliot A. Cohen, "Toward Better Net Assessment: Rethinking the European Conventional Balance," *International Security* 13, no. 1 (Summer 1988): 50–89. See also the exchange between Cohen and his critics in "Reassessing Net Assessment," *International Security* 13, no. 4 (Spring 1989): 128–79.

16. Jeffrey Lewis, "Yoda Has Left the Building," *Foreignpolicy.com*, 24 October 2014, http://www.foreignpolicy.com/articles/2014/10/24/yoda_has_left_the_building_andrew_marshall_pentagon_futurist.

17. Greg Jaffe, "U.S. Model for a Future War Fans Tensions with China and inside Pentagon," *Washington Post*, 1 August 2012, https://www.washingtonpost.com/world/national-security/us-model-for-a-future-war-fans-tensions-with-china-and-inside-pentagon/.

18. Andrew F. Krepinevich and Barry D. Watts, *The Last Warrior: Andrew Marshall and the Shaping of Modern American Defense Strategy* (New York: Basic Books, 2015), xviii.

19. For example, Douglas J. Feith, "The Hidden Hand behind American Foreign Policy," *Wall Street Journal*, 23 January 2015, http://www.wsj.com/articles/book-review-the-last-warrior-by-andrew-krepinevich-and-barry-watts-1422053324.

20. Desch, "Don't Worship at the Altar;" and Carlos Lozada, "Inside the Mind of the Pentagon's 'Yoda,'" *Washington Post*, 11 January 2015, http://www.washingtonpost.com/news/book-party/wp/2015/01/08/inside-the-mind-of-the-pentagons-yoda-3/.

21. The ONA will also continue: James H. Baker, a retired Air Force colonel who has been a strategist for the chairman of the Joint Chiefs of Staff, has been appointed to succeed Marshall as director of ONA. Thomas Gibbons-Neff, "Pentagon Chief Issues New Marching Orders for 'Yoda' Office," *Washington Post*, 10 June 2015, https://www.washingtonpost.com/news/checkpoint/wp/2015/06/10/pentagon-chief-issues-new-marching-orders-for-yoda-office/.

22. Richard A. Best Jr., *The National Counterterrorism Center* (*NCTC*)*—Responsibilities and Potential Congressional Concerns* (Washington, DCL Congressional Research Service, 19 December 2011), 4, https://www.fas.org/sgp/crs/intel/R41022.pdf.

23. Department of Homeland Security, "About the Domestic Nuclear Detection Office," 21 July 2015, http://www.dhs.gov/about-domestic-nuclear-detection-office.

24. Future of Terrorism Task Force, Homeland Security Advisory Council, Department of Homeland Security, *Report of the Future of Terrorism Task Force* (Washington, DC: DHS, January 2007), 6, http://www.dhs.gov/xlibrary/assets/hsac-future-terrorism-010107.pdf.

25. James Jay Carafano, Frank J. Cilluffo, Richard Weitz, and Jan Lane, "Stopping Surprise Attacks: Thinking Smarter about Homeland Security," *Backgrounder* no. 2016, Heritage Foundation, 23 April 2007, http://www.heritage.org/research/reports/2007/04/stopping-surprise-attacks-thinking-smarter-about-homeland-security.

26. Frank J. Cilluffo, "The Department of Homeland Security: An Assessment of the Department and a Roadmap for Its Future," statement before the US House of Representatives Committee on Homeland Security, 20 September 2012, 8, http://homeland.house.gov/sites/homeland.house.gov/files/Testimony%20-%20Cilluffo_0.pdf. More recently, Cilluffo repeated his call for an ONA within the DHS in commenting on the *Quadrennial Homeland Security Review*. See, Dan Verton, "DHS Releases Quadrennial Homeland Security Review," *FedScoop* (blog), 20 June 2014, http://fedscoop.com/dhs-releases-quadrennial-homeland-security-review/.

27. Office of the Press Secretary, White House, "Biodefense for the 21st Century" (press release, White House, 28 April 2004), http://www.fas.org/irp/offdocs/nspd/hspd-10.html.

28. Judith Miller, "Bioterrorism's Deadly Math," *City Journal* 18, no. 4 (Autumn 2008): http://www.city-journal.org/2008/18_4_bioterrorism.html.

29. Forrest and Hilliker, "Why the Department of Homeland Security," 2–3, 8, and 12.

30. James R. Clapper, director of national intelligence, "Current and Future Worldwide Threats to the National Security of the United States," remarks as delivered to the Senate Armed Services Committee, 11 February 2014, http://www.dni.gov/files/documents/WWTA%20Opening%20Remarks%20as%20Delivered%20to%20SASC_11_Feb_2014.pdf.

31. Gen Martin Dempsey, chairman of the Joint Chiefs of Staff, *Hearing to Receive Testimony on the Impacts of Sequestration and/or a Full–Year Continuing Resolution on the Department of Defense, Hearing before the US Senate Armed Services Committee*, 113th Cong., 1st sess., 12 February 2013, http://www.armed-services.senate.gov/imo/media/doc/13-03%20-%202-12-13.pdf.

32. Christopher A. Preble, *The Most Dangerous World Ever?* (policy report, Cato Institute, Washintgon, DC, September–October 2014), http://www.cato.org/policy-report/septemberoctober-2014/most-dangerous-world-ever.

33. Jeh Johnson, secretary of homeland security, *Written Testimony of DHS Secretary Jeh Johnson for a House Committee on Homeland Security Hearing on "Worldwide Threats to the Homeland,"* 17 September 2014, http://www.dhs.gov/news/2014/09/17/written-testimony-dhs-secretary-jeh-johnson-house-committee-homeland-security.

34. Jeh Johnson, secretary of homeland security, *Statement before the US House Judiciary Committee*, 113th Congress, 2nd sess., 29 May 2014, http://judiciary.house.gov/_cache/files/189c8334-81e9-4d5e-bf46-96e0383e6ee2/dhs-testimony-5.29.14.pdf.

35. At least one analyst has called for such work to be done: Adam Elkus, "Towards a Counterterrorism Net Assessment," *Small Wars Journal*, 21 December 2011, http://smallwarsjournal.com/jrnl/art/towards-a-counterterrorism-net-assessment.

36. The 2015 *National Security Strategy* describes guarding against terrorism as "the core responsibility of homeland security." Barack Obama, *National Security Strategy* (Washington, DC: The White House, February 2015), 8, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

37. Jeh Johnson, *The 2014 Quadrennial Homeland Security Review* (Washington, DC, DHS, 2014), 5, http://www.dhs.gov/sites/default/files/publications/2014-qhsr-final-508.pdf.

38. Office of the Press Secretary, White House, "Fact Sheet: The *2015 National Security Strategy*" (press release, White House, 6 February 2015), https://www.whitehouse.gov/the-press-office/2015/02/06/fact-sheet-2015-national-security-strategy.

39. Rose McDermott, "Methodology for Homeland Security," *Journal of Homeland Security and Emergency Management* 7, no. 2 (July 2010).

40. For example, Skypek, "Evaluating Military Balances through the Lens of Net Assessment," 6.

41. It is important to note that Clausewitz's discussion of the trinity is considerably more complex than simply the interaction of the people, the army, and the state. He described the components of the trinity as 1) primordial violence, hatred, and enmity; 2) the play of chance and probability; and 3) the subordination of war to rational policy. He went on to state that the first of these mainly concerns the people, the second the army, and the third the government, but scholars have argued that this shorter definition of the trinity is too simplistic or even wrong. For a discussion of this debate, see Edward J. Villacres and Christopher Bassford, "Reclaiming the Clausewitzian Trinity," *Parameters* 25, no. 3 (Autumn 1995): 9–19, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/1995/1995%20villacres%20and%20bassford.pdf.

42. I am grateful to Captain Todd Veazie, US Navy, for suggesting that Clausewitz's concept of the trinity can be helpful in understanding homeland security.

43. Business Executives for National Security (firm), *Domestic Security: Confronting a Changing Threat to Ensure Public Safety and Civil Liberties* (Washington, DC: Business Executives for National Security, February 2015), 8, http://www.bens.org/file/CounterterrorismReport.pdf.

44. Brian Michael Jenkins, Andrew Liepman, and Henry H. Willis, *Identifying Enemies among Us: Evolving Terrorist Threats and the Continuing Challenges of Domestic Intelligence Collection and Information Sharing* (Santa Monica, CA: RAND, 2014), http://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF317/RAND_CF317.pdf.

45. Recent studies that take such a broad approach and might serve as models for a homeland-security net assessment include Bruce Hoffman, "A First Draft of the History of America's Ongoing Wars on Terrorism," *Studies in Conflict and Terrorism* 38, no. 1 (2015): 75–83; and Peter Bergen, Emily Schneider, David Sterman, Bailey Cahall, and Tim Maurer, *2014: Jihadist Terrorism and Other Unconventional Threats* (Washington, DC: Bipartisan Policy Center, 23 September 2014), http://bipartisanpolicy.org/wp-content/uploads/sites/default/files/BPC%20HSP%202014%20Jihadist%20Terrorism%20and%20Other%20Unconventional%20Threats%20September%202014.pdf.

46. Bergen, et al., *2014: Jihadist Terrorism and Other Unconventional Threats*, 9.

47. Johnson, *Statement before the US House Judiciary Committee*.

48. New America Foundation, "Homegrown Extremism 2001–2015," *International Security* (web site), 2015, http://securitydata.newamerica.net/extremists/analysis.html.

49. Brian Michael Jenkins, *Al Qaeda after bin Laden: Implication for American Strategy* (Santa Monica, CA: RAND, 22 June 2011), 5, http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT365.pdf.

50. The Colorado Information and Analysis Center (CIAC), for example, was recognized as the *Fusion Center of the Year* in February 2010 for its support to the Najibullah Zazi terrorism investigation, and later CIAC provided information that helped lead to the arrest of a bombing suspect. See Homeland Security Blog Team, "Fusion Centers: Empowering State and Local Partners to Address Homeland Security Issues," *DHS* (blog), 18 July 2011, http://web.archive.org/web/20130524232705/http://blog.dhs.gov/2011/07/fusion-centers-empowering-state-and.html.

51. US Senate Committee on Homeland Security and Governmental Affairs, Permanent Subcommittee on Investigations, *Federal Support for and Involvement in State and Local Fusion Centers*, staff report (Washington, DC: Senate, 3 October 2012), 2.

52. Michael Price, *National Security and Local Police* (New York: Brennan Center for Justice, New York University School of Law, 2013), 3, https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPolice_web.pdf.

53. For a much more positive view on fusion centers than the Senate report noted above, see US House Committee on Homeland Security, *Majority Staff Report on the National Network of Fusion Centers* (Washington, DC: House, July 2013).

54. Jenkins, "Al Qaeda after bin Laden," 7.

55. Gregory Treverton, "Intelligence Test," *Democracy: A Journal of Ideas* 11 (Winter 2009): http://www.democracyjournal.org/11/6667.php?page=all.

56. Bailey Cahall, David Sterman, Emily Schneider, and Peter Bergen, "Do NSA's Bulk Surveillance Programs Stop Terrorists?" (policy paper, New America Foundation, Washington, DC, January 2014), https://www.newamerica.org/international-security/do-nsas-bulk-surveillance-programs-stop-terrorists/.

57. See for example, Christopher Hewitt, "Law Enforcement Tactics and Their Effectiveness in Dealing with American Terrorism: Organizations, Autonomous Cells, and Lone Wolves," *Terrorism and Political Violence* 26, no. 1 (2014): 58–68.

58. Peter Baker, "Obama Apologizes after Drone Kills American and Italian Held by Al Qaeda," *New York Times*, 23 April 2015, http://www.nytimes.com/2015/04/24/world/asia/2-qaeda-hostages-were-accidentally-killed-in-us-raid-white-house-says.html?_r=0.

59. Bergen, et al., *2014: Jihadist Terrorism and Other Unconventional Threats,* 47.

60. James J. Wirtz, "The Cyber Pearl Harbor," in *Cyber Analogies*, edited by Emily O. Goldman and John Arquilla (Monterey, CA: Naval Postgraduate School, 28 February 2014), 7–14.

61. Erik Gartzke, "The Myth of Cyberwar," *International Security* 38, no. 2 (Fall 2013): 41–73; and Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2011): 5–32.

62. Deborah Charles, "U.S. Homeland Chief: Cyber 9/11 Could Happen 'Imminently,'" *Reuters*, 24 January 2013, http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124.

63. Ellen Nakashima, "Cyber-Spying Said to Target U.S. Business," *Washington Post*, 11 February 2013.

64. James R. Clapper, *Worldwide Threat Assessment of the US Intelligence Community*, statement for the record before the Senate Armed Services Committee, 26 February 2015, 1.

65. Bergen, et al., *2014: Jihadist Terrorism and Other Unconventional Threats*, 43.

66. Colin S. Gray, *Making Strategic Sense of Cyber Power: Why the Sky is Not Falling* (Carlisle, PA: US Army War College Strategic Studies Institute, 2013), xi.

67. Clifton B. Parker, "Fight against Terrorism Likely Slow and Incomplete, Stanford Scholar Says," *Stanford News Service*, 3 September 2014, http://news.stanford.edu/news/2014/september/terrorism-strategy-crenshaw-090314.html.

68. Although the commander of USCYBERCOM is also the director of the NSA and the two organizations are both located at Fort Meade, Maryland, the two commands have different missions and operate under different legal authorities. See National Security Agency, "Frequently Asked Questions about NSA," https://www.nsa.gov/about/faqs/about_nsa.shtml#about10.

69. Quoted in Ellen Nakashima, "Dual-leadership Role at NSA and Cyber Command Stirs Debate," *Washington Post*, 6 October 2013, https://www.washingtonpost.com/world/national-security/dual-leadership-role-at-nsa-and-cyber-command-stirs-debate/2013/10/06/ffb2ac40-2c59-11e3-97a3-ff2758228523_story.html. See also Frank J. Cilluffo and Joseph R. Clark, "Repurposing Cyber Command," *Parameters* 43, no. 4 (Winter 2013–14): 111–18.

70. James Stavridis, "Why the Nation Needs a US Cyber Force," *Boston Globe*, 29 September 2013, https://www.bostonglobe.com/opinion/2013/09/29/why-nation-needs-cyber-force/quM4WWdJOh0FoSyE7rmxJI/story.html.

71. Richard Clarke, "Foreword," *Strategic Insights* 10, no. 1 (Spring 2011): 1, http://edocs.nps.edu/npspubs/institutional/newsletters/strategic%20insight/2011/SI_v10_I1_Spring_2011.pdf.

72. Aliya Sternstein, "Pentagon to Recruit Thousands for Cybersecurity Reserve Force," *Defenseone.com*, 16 April 2015, http://www.defenseone.com/technology/2015/04/pentagon-recruit-thousands-cybersecurity-reserve-force/110407/.

73. Eric Rosenbach, *Statement for the Record before the U.S. Senate Committee on Armed Services, Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., 14 April 2015. In July 2015, Rosenbach was named chief of staff to Secretary of Defense Ashton Carter. See also the recently released *DOD Cyber Strategy*, April 2015.

74. Michael S. Rogers, *Statement before the House Committee on Armed Services Subcommittee on Emerging Threats and Capabilities*, 114th Cong., 1st sess., 4 March 2015, 12.

75. David Clark, Thomas Berson, and Herbert S. Lin, eds., *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues* (Washington, DC: National Research Council, 2014), 100.

76. For example, a *Joint Action Plan for State-Federal Unity of Effort on Cybersecurity* was approved by the National Governors Association in July 2014. For an argument that city governments must take on more responsibilities in cyber security, see Mitchell D. Silber and Daniel Garrie, "Guarding Against a 'Cyber 9/11,'" *Wall Street Journal*, 16 April 2015, http://www.wsj.com/articles/guarding-against-a-cyber-9-11-1429138821.

77. Johnson, *2014 Quadrennial Homeland Security Review*, 21.

78. See for example The Centers for Disease Control and Prevention, "2014 Ebola Outbreak in West Africa," http://www.cdc.gov/vhf/ebola/outbreaks/2014-west-africa/.

79. Johnson, *2014 Quadrennial Homeland Security Review*, 22.

80. Ibid., 8.

81. Department of Homeland Security, *National Preparedness Report* (Washington, DC: DHS, 30 March 2014), http://www.fema.gov/media-library-data/1409688068371-d71247cabc52a55de78305a4462d0e1a/2014%20NPR_FINAL_082914_508v11.pdf.

82. See for example, Brian A. Jackson, *Applying Lessons Learned from Past Response Operations to Strengthening National Preparedness* (Santa Monica, CA: RAND, July 2014), http://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT411z1/RAND_CT411z1.pdf.

83. William O. Jenkins Jr., "Measuring Disaster Preparedness: FEMA Has Made Limited Progress in Assessing National Capabilities," Testimony before the Senate Committee on Homeland Security and Governmental Affairs, 17 March 2011.

84. Paul Stockton, "Ten Years After 9/11: Challenges for the Decade to Come," *Homeland Security Affairs* 7 (September 2011): https://www.hsaj.org/articles/582.

85. Thad W. Allen, "Confronting Complexity and Creating Unity of Effort: The Leadership Challenge for Public Administrators," *Public Administration Review* 72, no. 3 (May–June 2012): 320–21.

86. Christopher Dickey, "Time to Brace for the Next 9/11," *Newsweek*, 12 September 2011, http://www.newsweek.com/time-brace-next-911-67389.

87. Department of Homeland Security, *Fiscal Years 2014-2018 Strategic Plan* (Washington, DC: DHS, no date), 35, http://www.dhs.gov/sites/default/files/publications/FY14-18%20Strategic%20Plan.PDF.

88. Michael Chertoff "Remarks by the Secretary of Homeland Security Michael Chertoff" (speech, Bureau of Justice Assistance, Washington, DC, 14 March 2006), http://www.dhs.gov/xnews/speeches/speech_0273.shtm.

89. For a discussion of the civil liberties implications of domestic intelligence collection, see Erik J. Dahl, "Domestic Intelligence Today: More Security but Less Liberty?" *Homeland Security Affairs*, September 2011, https://www.hsaj.org/articles/67.

90. Bracken, "Net Assessment: A Practical Guide," 94.

Resiliency in Future Cyber Combat

Col William D. Bryant, USAF

The winds may fell the massive oak, but bamboo, bent even to the ground, will spring upright after the passage of the storm.

—Japanese proverb

Abstract

Rigid cyberspace defenses are proving unable to meet advanced and modern cyberspace threats. As a result, there has been increasing focus and interest in cyber resiliency, but what will it take to be resilient in future cyber combat? We can glean some useful concepts from the ancient Japanese proverb about the resiliency of bamboo in a storm. In comparison with the massive oak, which relies on structural strength, three characteristics enable the bamboo's greater resiliency. Bamboo has the ability to accept deformation without failure and a significantly reduced attack surface, and it dynamically reacts to the wind in a way that minimizes the impact of future gusts. Defenders of cyberspace should look to add similar characteristics to their cyberspace systems. First, cyberspace defenders should maximize the flexibility of their systems by deliberately building in "inefficient" excess capacity, planning for and expecting failure, and creating personnel flexibility through training and exercises. Second, defenders should reduce their attack surface by eliminating unnecessary capability in both hardware and software, resist users' desire for continual rapid improvements in capability without adequate security testing, and segment their networks and systems into separate defended enclaves. Finally, cyber defenders should position themselves to dynamically respond to attacks through improved situational awareness, effective cyberspace command and control, and

---

Col William D. Bryant is a career fighter pilot and strategist with a PhD in military strategy from the School of Advanced Air and Space Studies. He has served in numerous operational and staff assignments and is currently the deputy director of Task Force Cyber Secure on the Air Staff. His recently published book is titled *International Conflict and Cyberspace Superiority: Theory and Practice* (New York: Routledge, 2015).

active defenses. Combining these approaches will enable the defenders of cyberspace systems to weather cyberspace attacks and spring upright after the passage of the storm.

✳ ✳ ✳ ✳ ✳

According to the ancient Japanese proverb, after the storm passes, the stronger oak lies on the ground while the weaker bamboo stands upright. The moral that resiliency is more important to success than strength applies to conflict in the cyberspace domain as well. It is important to clarify that the resilience being discussed here is in response to cyberspace attacks, not cyberspace espionage. Cyberspace attacks change friendly systems through manipulating data, causing hardware failures, or physically destroying objects controlled from cyberspace. If pure cyberspace espionage is done well, the defenders will have no idea anyone was ever in their systems: everything will still function. Resilience is not as useful in examining cyberspace espionage as it is in investigating cyberspace attack.

The Department of Homeland Security's Risk Steering Committee has defined resiliency as the "ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption."[1] As organization after organization and system after system is successfully attacked, there is a growing realization that a perfect perimeter defense is not possible, and even if it were, attackers are often within the walls as insider threats. In addition, while shifting to multiple layers of "defense in depth" improves security, each layer will still have flaws and vulnerabilities that a determined attacker can circumvent. Accordingly, cyberspace operators have increasingly looked to resilience as a promising way to improve overall security.[2]

While resilience is the key to success for cyberspace defenders, it is important that defenders not neglect traditional network defenses. In the US military, the tendency has been to pour a disproportionate amount of resources into offense while not focusing enough on defense. This is a mistake, and as noted by Martin Libicki, "In this medium, the best defense is not necessarily a good offense; it is usually a good defense."[3] Offense is widely seen as overwhelmingly powerful over defense, but that assumption ignores the historical record of cyberspace attacks to date. Modest defenses easily defeat unsophisticated attacks, and even nation-state–level attacks have had mixed success. Of the eight cases of nation-

state on nation-state cyberspace attacks with a reasonable amount of open-source data, only half can be qualified as a success.[4] If the offense were truly so overwhelming, it should be able to achieve greater than a 50 percent success rate. When the high-level attacks are analyzed, it is apparent that in most cases the offenders did get past the defenses, but the defenders were able to react and negate the attacks in a week or two. Resilience is the key to an effective response.[5]

Before developing the tenets of cyberspace resiliency, it is important to clarify what cyberspace is, as there is great confusion on this point. The US Joint Staff has defined cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[6]

One important point emerging from the definition is that while the Internet is part of cyberspace, it is not all of cyberspace. Any computer processor capable of communicating with a computer system is in some way part of cyberspace. A desktop computer, an avionics computer on an aircraft, an iPhone, an industrial controller, and the central processor on a modern car are all part of cyberspace, although only some of them are routinely connected to the Internet. Most modern military equipment is more complex than an M-4 carbine and has some form of processor, from a humble truck to an aircraft carrier, and is thus part of cyberspace. So what is required to be resilient within cyberspace?

Using the bamboo analogy, there are three elements of success against the storm that have application to resiliency in the cyberspace domain: flexibility, a reduced attack surface, and the ability to respond dynamically to attacks. First, the bamboo can accept deformation without failure. As noted by the proverb, the bamboo can be bent and spring back upright, while the oak can accept little deformation before failing catastrophically. Second, the bamboo presents far less attack surface to the attacking wind, as it has a streamlined shape with relatively few exposed leaves compared to the oak tree, which has a far larger and more complex structure. Finally, the bamboo adjusts to the wind, bending to minimize the effect of future wind gusts. Each of these three characteristics can be applied to the cyberspace domain as a way of understanding how practical cyberspace resilience can be achieved.

Flexibility

What does flexibility look like in cyberspace? Is flexibility even a meaningful concept when every device in cyberspace is actually running a complex rule-set that predetermines its actions in response to a given set of inputs? While the computers that make up cyberspace simply do what they are told, the flexibility in cyberspace comes from people telling machines what to do. People can also build in more capacity for flexibility by constructing their systems to operate in cyberspace with excess capability.

The typical business mind-set focuses on efficiency to generate as much profit as possible, while the military mind-set loves both efficiency and order, but both concepts are antithetical to flexibility in cyberspace. Efficiency means using 100 percent of available resources with no excess capability. Yet, if you are 100 percent efficient, the smallest perturbation can lead to catastrophic failure. The heart of resiliency is the ability to absorb perturbations and failures—whether natural or manmade—and continue functioning. Thus, a system built for resiliency will look very different than one built for efficiency.

Too much efficiency will hamper resiliency, and cyberspace defenders would do well to build less-efficient redundant systems if they want to achieve resiliency under attack. Cyberspace operators who want to build a resilient system must oppose several efficiency trends. In the perfectly efficient network, every device on the network will run the same operating system, utilize the same applications for specific tasks, have a minimum of subnetworks or enclaves all structured the same way, and even utilize the same hardware throughout for the same functions. While these concepts are efficient, they are not resilient.

An entire network that runs a single operating system is efficient and easy to administer and also just as easy to take down via a single vulnerability. A heterogeneous network made up of Windows 7, Windows 8, and Linux—with a few Apple machines thrown in for good measure—cannot be completely taken down by a single vulnerability. Military strategist Edward Luttwak noted that in the strategic realm with a thinking enemy "homogeneity can easily become a potential vulnerability."[7] Of course, there must be a balance between efficiency and resiliency; a system where every single device runs a unique operating system would be resilient in a sense but would be so difficult to administer it would likely be full of unpatched machines and unknown

vulnerabilities. Aristotle taught that virtue always lies on a continuum between two vices.[8] The virtue of cyberspace resilience lies between rigid conformity to a single system that can be taken down with a single attack on one side and complete chaos within an unworkable mess of a network on the other. A reasonable middle ground for cyberspace operators is to select a handful of different, well-designed operating systems and then implement them throughout their networks. Thus, if three operating systems are used, two-thirds of the network should be available following any attack that uses a single vulnerability. Cyberspace operators should also find the right balance between too many and two few different types when it comes to applications and hardware, for very much the same reasons as discussed above for operating systems. Heterogeneous systems are a start, but the defender can also break those systems into separate enclaves to further increase resiliency.

Network segmentation into separate subnetworks that can function even if other networks around them fail is a key component of cyberspace resiliency. The current push toward ever-larger homogenous networks is good for efficiency but not for resiliency. Consider the changes the network on a typical military base has gone through. At first, every base was unique; information technology (IT) equipment was purchased locally, and every network ran different software and applications depending on what the local communications unit purchased. This structure was extremely inefficient, and the level of security achieved was highly variable and often quite low—partially because the different networks still had to be connected to each other, often in not very secure ways. The next step was to bring control of the networks up to a regional level, which took control of base networks largely out of the hands of local units. While this resulted in a more efficient network, it also meant a successful attack against the regional hub could bring down multiple bases at the same time, whereas before, each base would have to have been reconnoitered and attacked separately. Now, the Department of Defense (DOD) has mandated that the military services all utilize the same structure under the Joint Information Enterprise and the same network hubs in the form of Joint Regional Security Stacks. If every service is using the same equipment running the same software, one successful attack against a single vulnerability could conceivably take down the entire DOD network.

Returning to the "Wild Wild West" mind-set, where every local unit does whatever it wants, will not improve operational effectiveness. Instead, resiliency and a reasonable level of efficiency can be achieved by a deliberate diversification of networked systems. Homogeneity is good for ensuring patches and protocols are followed against known threats, while heterogeneity helps protect a system from unknown and unpredictable threats. System architects should buck the trend toward ever-larger and homogenous networks and deliberately build in heterogeneous enclaves based on a small number of carefully selected hardware and software configurations. It is important that network architects do not build systems with a single type of system performing a function across the network. For example, a segmented network of heterogeneous enclaves that all use the exact same hardware and software as a gateway will be less resilient than one that uses different types of gateways. Resiliency is best increased by parallel lanes of different systems, if a network relies on a single type of system at any level, there is still a single point of failure. As with operating systems, finding Aristotle's "golden mean" of enough diversification to be resilient with enough efficiency to be manageable and low-cost is the key.

Even if a network is heterogeneous and cannot be completely taken down by a single vulnerability, cyberspace operators still need to expect and plan for failure.[9] Planning for failure does not come naturally, especially in the military environment. Complexity theorist Antoine Bousquet has noted that the military often attempts to achieve "100% relevant content, 100% accuracy, and zero time delay" in the pursuit of a frictionless cybernetic war machine, but that goal is illusory. Instead, cyberspace operators should be "embracing uncertainty and designing a resilient and flexible military that is capable of adapting to the unforeseen and contingent."[10] Cyberspace operators need to move beyond the concern of how to best secure their systems against attack to focus on how to design their system to continue working after their defenses fail. This requires a significant mind-set shift for military cyberspace operators, including focusing on response capabilities such as emergency and incident response teams and plans.[11] One of the best ways to accomplish this shift is through aggressive and thorough red teaming.

Well-resourced and extensive red teaming of cyberspace systems is a critical part of building cyberspace resiliency. A red team is a group of friendly attackers who attempt to attack systems to find their vulner-

abilities and weaknesses. They use the same techniques as real attackers and provide an invaluable service in not only finding vulnerabilities but also giving defenders practice in how to respond to attacks and keep their systems functioning. To get the maximum benefit out of red teaming, exercise referees need to allow red teams to breach defenses and actually do damage within the exercise system; stopping the exercise when the red team gets access does not yield as much benefit. Historically the DOD has underresourced red teams due to the persistent focus on offensive cyber capabilities. Red teams require the same people and resources needed for offensive cyberspace capabilities. However, offensive capabilities and red teams are not locked in a zero-sum resource game. Since the same attack techniques are used, red teaming can be excellent training for offensive cyberspace operators and can help overcome classification barriers.

Compartmentalization continues to be a major issue preventing defenders and attackers from learning from each other.[12] According to former vice-chairman of the Joint Chiefs of Staff, Gen James Cartwright, "We make sure the recce teams don't tell the defenders what they found, or the attacker, and the attackers go out and attack and don't tell anybody they did. It's a complete secret to everybody in the loop and it's dysfunctional."[13] Compartmentalization and security are essential in protecting cyberspace weapons, but it is foolish for attackers to assume their enemies will not discover and utilize the clever techniques they develop. Attackers need to inform friendly defenders of their attack methods in appropriate ways that allow defenders to defend their systems, while not giving away the attack methods to adversaries. Once again, there is a balance required between disclosure and security, but it appears in the DOD the needle is too far toward security. More disclosure by attackers to defenders is needed for improved cyberspace resiliency. Red teaming and improved disclosure helps to develop resiliency in the people operating in cyberspace, but there are a number of other ways to build resiliency into cyberspace operators.

The highest payoff in building cyberspace resiliency lies in building resilient people. People, not machines, react. The machines will simply do what their instructions tell them to do, even if those instructions are complex and allow for some ability to respond to stimuli. Not only do cyberspace operators need to be resilient, improved resiliency and security needs to be built into system users as well.

Education that creates deeper understanding of the cyberspace environment will often yield a major payoff in unexpected ways and places. Training is valuable and can produce an immediate payoff; education takes longer but can provide more benefit in the long run. Because of the long-term and difficult-to-measure nature of the payoff, education often takes the first hit when an organization is under budgetary pressure. This is shortsighted and will reduce an organization's abilities to understand the environment and to generate the cultural change needed to build an organization that can be resilient in the cyberspace domain. Education lays the foundation, but training provides the specific tools needed by people operating in cyberspace.

Users can be "hardened" via training, as they are currently the weakest spot in the armor of most cyberspace systems. Users are the bane of system administrators the world over, and many attacks rely on finding a user who can be tricked into compromise. Most users have only a rudimentary knowledge of computer security, so spending time and money training them can produce a significant payoff. Mandatory training programs are a start, but not all users will pay attention to training or be convinced that it is important to them. System administrators need to convince users there is a significant benefit to following good security practices, whether it is monetary rewards for best practices or reprimands for those who do not follow procedures.

Most organizations have a user training program in place; what is missing is accountability to make users take cyberspace security seriously. In a recent study, security testers left USB thumb drives on the ground in a parking lot outside of a federal office building. All federal employees receive regular training on the dangers of plugging in unknown USB devices, but 60 percent of these highly trained employees plugged them in anyway. The addition of an official looking logo on the drive increased the percentage of USB drives employees plugged in to 90 percent.[14] How many of these employees were fired or even mildly reprimanded for their failure to follow procedures? Performance ratings and rewards need to be explicitly tied to following security practices, and there should be consequences for security failures that are regularly tested via a continuing testing program.

Users should be routinely tested and probed, and those who do not perform well should face escalating consequences. For example, cyberspace operators should routinely send out "phishing" style e-mails to users

of their systems based on actual real-world attacks. If a user is duped into clicking on the link, instead of unleashing a virus, the user should be directed to retake the organization's computer security training. Subsequent failures should have increasingly unpleasant consequences, including eventual termination for employees who are incapable of following good security practices. A similar escalation ladder could be followed for users who continue to visit questionable sites or are caught deliberately circumventing security safeguards. Escalating consequences are for well-intentioned but security inept employees; insider threats are a different matter and should be dealt with according to organizational and legal rules. These types of changes will normally not be received well because they involve changing organizational culture and they will require support from top executives in the organization to be successful. For the military in particular, cyberspace resilience will also include a significant amount of resilience outside of cyberspace systems.

For most Western militaries, cyberspace systems are principally important because they enable effectiveness in the physical domains of combat. Thus, cyberspace resilience includes the ability of military forces to fight effectively even if their cyberspace systems are compromised or unavailable.[15] Management scientist Martin Libicki has recently identified that networked militaries need to be careful not to focus on the network for its own sake through information assurance but must instead stay focused on the mission and mission assurance.[16] This is deeply uncomfortable for a generation that has become accustomed to continual connection and reliability of cyberspace systems, since Western militaries have not yet fought a significant cyberspace adversary. However, there are a number of potential adversaries who have been very clear that they intend to fight hard in cyberspace in the case of a conflict, and Western militaries would be exceedingly foolish to assume the enemy will never have a "good day" and be able to disrupt many critical systems.

Much like with cyberspace operators and system users, resilience in regular military forces can best be built through realistic training and exercises. Currently, if there is cyberspace play in military exercises, exercise referees usually discount it so regular forces can receive "good training" and utilize all their systems. On the contrary, *good training* is when they do not have all their systems. Consider a single cyberspace enabled system, the Global Positioning System (GPS). What would a major exercise such as Red Flag look like if none of the participants were

allowed to use GPS? What about a land-based combat exercise at the National Training Center? How many young platoon leaders would be able to maneuver their forces quickly and expertly using only a compass and a map? What if their radios stopped working as well? Would forces continue to maneuver and operate in the absence of communication from headquarters? There are some hopeful signs that some leaders in the military are taking this threat seriously, and distributed control is one promising approach.[17] But these ideas must be thoroughly tested and exercised on a regular basis if military forces are going to have any ability to operate in a cyberspace-denied environment. The flexibility created by these changes can be enhanced by also reducing a cyberspace system's attack surface.

Reducing Attack Surfaces

Bamboo has far less surface area in its structure than the massive oak tree and thus presents a much smaller surface for the wind. In cyberspace, the surface area is normally referred to as the "attack surface." The attack surface is made up of all the potential access points for an attack. Cyberspace operators should actively seek to make their attack surface as small as possible so the effect of each attack and the resultant recovery time are minimized. The fewer systems that must be recovered, the more quickly recovery can take place.

Every piece of software, every capability added to that software, and every communications pathway represents a potential avenue of enemy attack. Thus, the first thing cyberspace operators should do to reduce the attack surface they present to the enemy is eliminate nonessential features, as such features represent added risks.[18] This is a mammoth task—one most cyberspace operators are not easily able to accomplish, as modern software is written to appeal to the largest number of customers with all the bells and whistles on by default. It can be nearly impossible, not only to determine what functionality is unneeded but also to disable it across the network to prevent it from being used as an attack vector. While swallowing the elephant all at once is not immediately achievable, concrete steps can be taken in both the software and hardware arenas.

An organization's hardware attack surface can be reduced by disabling unnecessary ports and communications pathways where possible. The best method for disabling unnecessary communications pathways is

via physical means. If a computer's wireless network or modem card is removed, there is complete certainty that card cannot be used as a clandestine back door into the organization's network. The same can be said for unnecessary physical connections such as USB ports. It may be inelegant to cut the wire behind the port, or fill the port opening with hot glue, but it is effective. Software methods can be used as well, even if they are not as effective. Most devices can be easily disabled via the operating system, although cyberspace operators would do well to run periodic checks to ensure disabled ports have not been turned back on surreptitiously. While closing hardware-based vulnerabilities is a start, the majority of an organization's attack surface lies in its software.

If an organization is serious about its cyberspace security, there should be an increased level of scrutiny of every piece of software on the organization's networks. As with operating systems, there must be a balance between having too many and too few different applications to accomplish the same function. Having too many applications opens unnecessary avenues of attack, while having too few can hamper resiliency. For example, if an organization mandates the use of only one particular build of one Internet browser, it is difficult for the organization to react quickly if a vulnerability is discovered in that browser. If the same organization had two browsers on the network, all functionality could be quickly switched to the second browser while the first was patched. However, in many networks there are clearly far too many applications, not too few. It is reasonable to have a primary and a spare application for each function, but not reasonable to have 12 applications that do the same thing. Of course, a system administrator telling users they cannot utilize their favorite application is about as popular as the Internal Revenue Service auditor. The importance of reducing an organization's attack surface presented via too many applications is not well understood. Users will often push back against security requirements if it means they cannot get the software they want as quickly as they want to get it.

There is a natural tension between the desire of users for continual connection with constant improvements and security requirements to restrict unnecessary communications pathways and comprehensively check all new software. Once again, balance is the key, and cyberspace operators must find the correct balance between competing requirements. That balance will be different for each organization and operational environment. The right balance for a small IT firm developing

iPhone applications is very different than the right balance for the National Security Agency (NSA). Once an organization has done all it can to reduce its software and hardware attack surfaces, it can take one more step.

The final step in reducing the attack surface shown to a cyberspace attacker is to hide as much of it as possible behind different segments of the network. In many respects, this is very similar to a "defense in depth," where once the attackers get over one wall, they are faced with a whole new series of walls different than the first.[19] These additional barriers can also provide more opportunities for the defender to detect the attack. There is some overlap with the previous discussion on flexibility, as segmentation can aid flexibility and also reduce an organization's apparent attack surface. True, air gaps remain very difficult to maintain without some connection for maintenance or communication, but segmenting a network into different areas with strictly controlled communication links can reduce an organization's attack surface. The amount of communication allowed into or out of the segments can be adjusted to account for the level of security required. The control system for a nuclear power plant should have very little and strictly controlled access to communication flows, whereas the segmented network for an operating division inside a corporation will normally have much freer communication links.

The key to reducing attack surfaces appropriately is finding the right balance between connectivity and security. However, the world is full of aggressive actors in cyberspace, and it is likely an attacker will find a vulnerable attack surface eventually. Then the flexibility an organization has built will be tested as it reacts to the storm and bends like the bamboo.

Reacting to Attack

When bamboo bends during a storm, it is in response to the pushing of the wind. The bamboo bends away from the wind, which reduces the amount of the bamboo's surface the wind can push on, and the bamboo's leaves and branches streamline, which reduces the force on the bamboo even more. If cyberspace operators are going to react to attacks in an analogous way, they must start by understanding what is going on around them in cyberspace.

Cyberspace situational awareness is normally essential for cyberspace operators to effectively react to an attack. Defenders must know they are under attack before they can react resiliently. If an attacker is simply trying to steal information or implant pathways for future attacks, he or she may work very hard to avoid detection. Resilient cyberspace defenders must find the enemy to affect a response, but to find the enemy, defenders first must know their own home terrain.

Cyberspace situational awareness starts with the cyberspace defender; cyberspace operators need to understand their own networks. This point at first may seem so obvious as to be hardly worth stating, but it may surprise people outside the IT industry that many large organizations—including the military services—do not have a complete picture of what their networks look like, exactly how and to what they are connected, or even what applications are running on their networks. Large amounts of money are being spent to attempt to solve this problem, but an immediate solution is not apparent. Automated tools do a good job finding what they know to look for, but unique systems and applications are often missed, as the automated tools do a poor job of finding and categorizing unknown software. Legacy networks can be riddled with "servers" that are actually desktop computers sitting under a desk somewhere that were configured years ago to do a specific task that may, or may not, still be required. Once a picture of your own network is built, the next step is to consider what the enemy may be trying to do to it.

Intelligence on cyberspace threats is extremely difficult to collect. Cyberspace weapons are easy to build in extreme secrecy, as the resources needed to create them can be easily hidden compared to the resources required to build a battleship or bomber. Intelligence agencies should pursue information on cyberspace capabilities and intentions, but much of their best work will likely not be via cyberspace but via other, more traditional methods, since people drive cyberspace. Moreover, people may yield better intelligence than computers and networks in this area. Consider for a moment the presumed difficulty a nation-state would have hacking into the NSA compared to how easy it apparently was for Edward Snowden to walk out with an enormous amount of information. Once intelligence has been collected, via whatever means are available, cyberspace operators must overcome their own organization's security policies if it is to have any real effect.

While cyberspace weapons are very vulnerable to compromise and must be protected to be successful, the current extreme levels of secrecy hamper cyberspace resilience. Cyberspace capabilities were developed in a world steeped in high levels of classification and compartmentalization, and it is true that cyberspace weapons are very frangible. Once an enemy knows about an exploit or technique, the target can normally block it very quickly.[20] However, a better balance between security and strengthening defenses needs to be struck in this area. Cyberspace attackers should not have to share the details of their latest weapons and techniques, but they should provide generalized threat information based on friendly weapons for the benefit of their own cyberspace defenders. While an enemy might not use identical weapons, similar attacks might be thwarted. For cyberspace attackers to assume their enemy could not possibly be smart enough to discover the same vulnerabilities and techniques would be extremely foolish. Senior leaders who can balance improved defenses against possible loss of offensive capability will have to strike the right balance in this area. Sometimes the answer will be to disclose, and sometimes the offensive capability will be so important that the risk to friendly networks of leaving them unpatched will be deemed acceptable. Right now, it appears the default is that offensive forces share very little with their defensive brethren. For most organizations, Aristotle's golden mean appears to lie in the direction of more disclosure, not less. The next quandary for cyberspace operators is how to effectively command and control cyberspace forces.

Resilient operational cyberspace organizations should be commanded and controlled more like maneuver forces in the physical domains than managed as IT departments. Despite protestations by some analysts that there is no maneuver in cyberspace, humans, who make decisions and react to their adversaries in ways that would still be familiar to Carl von Clausewitz and other military thinkers, continue to drive conflict in the cyberspace domain.[21] Attempting to reduce military conflict to an engineering problem was a bad idea in the physical domains. Why would we expect it to be a good idea in cyberspace? Accordingly, structuring cyberspace forces as maneuver units that are expected to react and maneuver to defeat a thinking and reacting adversary is a good start. Currently, cyberspace command and control is also far too complex, with decisions to employ too far up in the chain of command and examined by too many different teams of lawyers. Streamlining the process is important,

but that will likely take time, as understanding of the cyberspace domain continues to develop. Meanwhile, maneuver and counterattack will remain important tools for resilient defenders.

According to Clausewitz, defenders should not simply wait passively; "the defensive form of war is not a simple shield, but a shield made up of well-directed blows."[22] William Owens, Kenneth Dam, and Herbert Lin demonstrated that with only a passive defense the defenders have to succeed every time, and since there are no penalties for the attacker, he can continue attacking until he is successful. This difference places "a heavy and asymmetric burden on a defensive posture that employs only passive defense."[23] A defender can be attempting to accomplish several things when counterattacking in cyberspace. A defender can disable the computers executing the attack and attempt to trace an attack back to its source. Attackers will normally bounce attacks through multiple servers to attempt to hide themselves, but a persistent defender can sometimes work back through the servers to the source or use more creative methods to identify the attacker. If a defender makes it to the originator of the attack, there are now a number of unpleasant things he or she could theoretically do to the attacker's networks in retaliation. Unfortunately, most of those things are currently illegal for defenders to do under US law.

Since active defense normally involves breaking into a number of privately owned computers along the way, it is generally illegal under the Computer Fraud and Abuse Act. According to Paul Rosenzweig, any active defense that reaches outside of the defender's computer system is "almost certainly a crime in and of itself."[24] This legal issue opens cyberspace defenders up to prosecution and lawsuits, whether they are military or civilian. And that is just if the attacking computers are only in the United States, which is normally not the case. Breaking into computers in foreign countries brings on entirely new sets of legal and political problems. The difficulty in attributing attacks might work in the defender's favor, as it can be hard to attribute "hack backs" if the defender chooses to mask where he or she is coming from, but that does not actually deal with the legal and ethical issues. Hack backs quickly devolve into a legal and political Gordian knot. Hack backs are a key element in an effective defense, but they are clearly illegal. However, it is just as clear that even private organizations are now using them.[25] Hopefully, policy and legal authorities will catch up in this important

area. Fortunately for defenders, there are other types of active defenses that pose fewer legal issues.

A less legally problematic technique a resilient cyberspace defender can use against an attacker is a "honey net," which diverts attackers into a false network full of whatever the defender wants the attacker to see. If a cyberspace attacker is attempting to break into a highly classified system and the defenders know it, they can divert the attacker into a false network. Having blocked the attacker, there is nothing preventing him from trying again using a different access that the defender might miss. If the defender instead diverts the attacker but provides him with false information, it can be far more effective. For the defenders to be effective in their deception, they must understand the expectations of the attacker and provide an environment tailored to what the attacker expects to find.[26] Something similar to this may have happened in the early 1980s when a US spy provided information the Soviet Union was planning to secretly acquire gas pipeline technology. Instead of blocking the sale, the United States allegedly quietly altered the computer code that eventually led to "the most monumental non-nuclear explosion and fire ever seen from space."[27] Defenders can do much the same thing in cyberspace. Once a defender captures an attacker in a honey net, the defender can keep the attacker busy with false information, examine attack patterns and techniques, embed beacons to phone home in the data that the attacker is taking, or carry out whatever other countermeasures are most useful. One of the most worthwhile techniques for a defender is instilling doubt in the mind of the attacker.

Introducing doubt into the mind of an attacker is one of the more useful things a resilient cyberspace defender can do with a honey net. A defender does not have to falsify everything; successfully falsifying one piece of information can make the attacker doubt everything else he or she got as well. One way of accomplishing this increased doubt is through a defender falsifying battle damage assessment (BDA). It is normally difficult for an attacker to understand how effective her or his attacks have been; a honey net can make it even worse. A defender can use a honey net to make it look like an attack has been successful, but then suddenly turn the system back on to ambush the attacker's forces at the most opportune time.[28] Tricking the enemy this way once will also have the effect of making the enemy very reluctant to trust any future cyberspace BDA. If an adversary does not fall for a honey net,

a resilient cyberspace defender should have multiple copies of critical data available.

Backups enable a defender to rapidly reconstitute damaged systems and data and provide a way for defenders to minimize the effect of even a successful attack.[29] An attacker who breaks into a logistics system and erases all the data can cause significant problems for a defender. However, if the defender has a backup and can have the system restored and operating in a day, the defender can minimize the attack's long-term effects. One of the hopeful trends for cyberspace defenders is the decreasing cost of electronic data storage. This decreasing cost makes it far easier for defenders to keep multiple copies of the data needed to restore a system. Of course, defenders need to keep the copies in a manner that prevents an attacker from getting to the backups and the primary system at the same time.[30] Automatic backup systems may be convenient, but they are automatic and will copy a cyberspace weapon just as easily as valid data. Backups are part of resilience, but cyberspace defenders can also build hidden additional capability into their networks.

A war reserve mode (WARM) is a concept from electronic warfare that has great applicability in cyberspace combat. Electronic warfare equipment, such as radars or radios, is often built with additional functionality that is not used unless needed in a major conflict against a top-tier enemy. The reason for these hidden modes is that every technique has a countermeasure, and if all of a combatant's techniques are used routinely, the enemy will find out what they are and develop countermeasures. If the best techniques are hidden and not used until combat starts, it can give one side a decisive advantage.

Applied to cyberspace, WARM would suggest that defenders have preplanned ways to significantly alter not only their defenses but also their networks in ways that make an attacker's careful reconnaissance obsolete. As Gregory Rattray, a former US Air Force commander for information warfare and a cyber expert at the National Security Council, has stated, in cyberspace the equivalents of mountains and oceans can be moved with the "flick of a switch."[31] Additionally, defenders do not have to accept the geography of their environment; they can actively change the terrain to make it harder to attack.[32] Cyberspace attackers often have to spend significant time and effort mapping out exactly how a network is configured and what software it is running. If a defender was to change all the software on his routers to a previously unknown

version just as a conflict starts, it could disrupt many of the attacker's plans. The new software does not even have to be better than the old one or have less vulnerabilities. The new vulnerabilities will still have to be discovered, which can buy the defender significant time and breathing space. The same principle could be utilized for any software on the network and even has applicability to hardware.

A well-resourced defender could have significant spare hardware of different types on hand to enable a quick rebuild of the network. For example, if a defender has a diversified network, with three types of routers, if one of those routers is successfully attacked, the defender could replace the vulnerable one with one of the other two types from storage. Defenders could go so far as to build entire networks using different types of hardware that are then left in a standby mode and disconnected from other systems, which makes them very difficult to attack. If the primary system is successfully attacked, the defender can switch to the backup. Defenders cannot simply set up a backup system and assume it will work when needed; they have to extensively test and evaluate it. Otherwise, a backup system may be useless, as it provides a false sense of security but no capability when it is needed.

Of course, setting up an entire backup network is extremely expensive and will likely only be worthwhile on a small scale and when the information or network is so critical that it cannot be allowed to fail. Nuclear command and control is one obvious area where the requirement for surety is so high that a complete backup network is reasonable. These techniques of improved situational awareness, effective command and control, hack backs, honey nets, backups, WARM, and backup networks will help cyberspace defenders dynamically maneuver and bend in the right direction when the attacking wind comes.

Conclusion

There are many ways cyberspace defenders can bend under attack before springing upright like the bamboo in the Japanese proverb. The three different elements that apply to the resilience of the bamboo as well as resilience in cyberspace are flexibility, reducing attack surfaces, and reacting dynamically to attack.

Flexibility in cyberspace conflict will largely stem from creating flexible people, although good network design that allows flexible cyber-

space operators more options will also help. Flexibility in cyberspace systems will be expensive, and efficiency will be lowered due to the necessary excess capacity that must be built into a more flexible system. A flexible cyberspace system is also one that is heterogeneous and broken into defensible enclaves, not one large and easy to administer network running the same software on every device. Flexible cyberspace personnel are best grown through extensive education, training, and exercises, including red teaming, full-scale exercises with cyberspace play allowed to affect the physical domains, and accountability for users who prove unable to adopt good security practices. Many of these changes will be very hard to implement, as they will be extremely uncomfortable to bureaucratic organizations and will require significant cultural change.

Reducing attack surfaces is the second element to creating cyberspace resiliency. The first and extremely difficult step is to eliminate unnecessary capability across the network, both in software and in hardware. Users will be discomfited by having to use different tools than they are used to, but the payoff in security can be significant. Not every backup system should be eliminated. Wherever possible, a primary and backup for each key mission area should be available to allow cyberspace operators to rapidly shift from one to the other if vulnerabilities are discovered. Users' desire for continual rapid improvements in communication and capability will also have to be balanced against security requirements, as each new capability or communications pathway introduces a potential attack vector. Striking the correct balance between security and capability will be a difficult and continuing challenge, and the correct balance will change depending on the organization and environment within which it operates.

The final element of resiliency in cyberspace is the ability to react dynamically to attack. Cyberspace operators need to develop better situational awareness of their own networks and develop intelligence capabilities to understand what the enemy is planning. Attackers and defenders on the same side also need to lower the walls between them and share more information to enable cyberspace defenders to be better able to defend their networks, while protecting offensive capabilities. Effective cyberspace command and control that treats cyberspace operators as maneuvering forces to be commanded versus an IT management problem with an engineering solution is also important. Active defenses,

including honey nets, backups, WARM, and backup hardware contribute to cyberspace resilience.

For an organization to create enduring cyberspace resilience, some aspects of all three elements will be required, and building in cyberspace resilience will not be cheap. The additional costs incurred for redundancy and training alone will overwhelm any potential savings from streamlining and reducing excess capacity. However, if an organization is serious about protecting its ability to accomplish its mission in cyberspace, resilience under attack will be the key. If cyberspace operators and their defended networks and systems adopt the characteristics of the versatile bamboo, they too will be resilient enough to spring upright after the passage of the storm. SSQ

Notes

1. Risk Steering Committee, *DHS Risk Lexicon: 2010 Edition* (Washington, DC: Department of Homeland Security, September 2010), 26, http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf.

2. Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York: Oxford University Press, 2013), Kindle location 720. Singer and Friedman have recently suggested that the classic information security "CIA Triad" of confidentiality, integrity, and availability should be extended to include resilience.

3. Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, CA: RAND Corporation, 2009), 176.

4. William D. Bryant, "Cyberspace Superiority: Dominating the Digital Frontier" (PhD diss., School of Advanced Air and Space Studies, 2014), 205.

5. Bryant, "Cyberspace Superiority," 206. I was only able to examine and code eight cases, due to limitations in the available unclassified data. The four successful cases in descending order of the level of success were Russia v. Georgia in 2009, the Nonghyup bank attack in 2011, Stuxnet, and the South Korean distributed denial-of-service (DDoS) attack of 2011. The four unsuccessful cases in decreasing order of the level of success were Russia v. Estonia in 2007, Aramco in 2012, the 2013 bank and media company attacks against South Korea, and North Korea's 2009 DDoS attack against the United States and South Korea. The evidence and measurement methodology supporting this coding can also be found throughout my cited dissertation.

6. Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*, 27 November 2012, II-9.

7. Edward N. Luttwak, *Strategy: The Logic of War and Peace* (Cambridge, MA: Belknap Press, 2003), 39–40.

8. Aristotle, "Nicomachean Ethics," in *The Book of Virtues*, ed. William J. Bennett (New York: Simon & Schuster, 1993), 102.

9. Paul Rosenzweig, *Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World* (Santa Barbara, CA: Praeger, 2013), Kindle location 3727.

10. Antoine Bousquet, *The Scientific Way of Warfare* (New York: Columbia University Press, 2009), 222.

11. Gregory J. Rattray, *Strategic Warfare in Cyberspace* (Cambridge, MA: MIT Press, 2001), Kindle location 220.

12. David J. Lonsdale, *The Nature of War in the Information Age* (London: Frank Cass, 2004), 154.

13. Gen James E. Cartwright, US Marine Corps, comments, Air Force Association Air Warfare Symposium, 8 February 2007, reported in Franklin D. Kramer, "Cyberpower and National Security: Policy Recommendations for a Strategic Framework," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 14.

14. Rosenzweig, *Cyber Warfare*, Kindle location 815, chap. 3.

15. Rattray, *Strategic Warfare in Cyberspace*, Kindle location 219.

16. Martin C. Libicki, "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8, no. 2 (Fall 2012), 330.

17. Gilmary Michael Hostage III and Larry R. Broadwell Jr., "Resilient Command and Control: The Need for Distributed Control," *Joint Forces Quarterly* 75, no. 3 (2014): 38–43.

18. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, DC: National Academies Press, 2009), 84.

19. Jeffrey Carr, *Inside Cyber Warfare: Mapping the Cyber Underworld* (Beijing: O'Reilly Media, 2011), Kindle location 3674.

20. Libicki, *Conquest in Cyberspace*, 74.

21. Carl von Clausewitz, *On War*, edited and translated by Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 75.

22. Ibid., 357.

23. Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 13.

24. Rosenzweig, *Cyber Warfare*, Kindle location 2024, chap. 7.

25. Kelly Jackson Higgins, "Free 'Active Defense' Tools Emerge," *Security Dark Reading*, 11 July 2013, http://www.darkreading.com/intrusion-prevention/free-active-defense-tools-emerge/240158160.

26. Colin S. Gray, *Modern Strategy* (New York: Oxford University Press, 1999), 35.

27. Thomas C. Reed, *At the Abyss: An Insider's History of the Cold War* (New York: Ballantine Books, 2004), 269. Other authors, such as Thomas Rid, have questioned whether the explosion actually occurred. Reed, given his various government positions, including Secretary of the Air Force, was in a good position to know of the events if they occurred as alleged. See Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2013), Kindle location 275.

28. Owens, Dam, and Lin, *Technology, Policy, Law, and Ethics*, 125.

29. Libicki links the replicability of cyberspace with its reparability in *Conquest in Cyberspace*, 5.

30. Singer and Friedman, *Cybersecurity and Cyberwar*, Kindle location 3177.

31. Gregory J. Rattray, "An Environmental Approach to Understanding Cyberpower," in *Cyberpower and National Security*, edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: Potomac Books, 2009), 256.

32. Libicki, "Cyberspace Is Not a Warfighting Domain," 324.

China-India

Regional Dimensions of the Bilateral Relationship

Chietigj Bajpaee

Abstract

While the Sino–Indian relationship has improved in recent years, it continues to oscillate between periods of cordiality and competition. This is exacerbated by a fundamental mismatch of threat perceptions between both states, rooted in the shifting balance of power and conflicting signals in the bilateral relationship. Moreover, the rise of both countries as major powers has provided them with new tools and platforms to interact with each other, contributing to a spillover of the Sino–Indian relationship from the bilateral to regional levels. Nowhere is this spillover effect or "nested security dilemma" more evident than in the maritime domain—amid the rise of both countries as major trading and resource-consuming powers. After charting the evolution of the Sino–Indian relationship, this article examines the implications of the changing nature of the Sino-Indian relationship on Asia's expanding strategic geography and US policy making toward Asia.

✳ ✳ ✳ ✳ ✳

The year 2014 marked the sixtieth anniversary of the signing of the "Five Principles of Peaceful Coexistence" between China and India on 29 April 1954.[1] The signing of this agreement marked the pinnacle of relations between the countries. However, within a decade the bilateral relationship reached its lowest point during a brief border war in 1962.[2] The fact that there has been no renewed outbreak of hostilities between China and India in the half century since the war is a positive achieve-

Chietigj Bajpaee is a doctoral candidate in the Department of War Studies at King's College London. He has worked with the Center for Strategic and International Studies in Washington, DC and the London-based International Institute for Strategic Studies. Bajpaee holds a master's degree in international relations from the London School of Economics.

ment. Aside from a few brief conflagrations, notably in Sikkim in 1967 and the Sumdorong Chu Valley in 1987, bilateral tensions have been confined to rhetoric and symbolic posturing.[3]

Nonetheless, while bilateral relations have improved, they continue to oscillate between periods of cordiality and competition. An underlying climate of mistrust continues to permeate the bilateral relationship—rooted in their unresolved border dispute. This is exacerbated by a fundamental mismatch of threat perceptions between both states, rooted in the shifting balance of power and conflicting signals in the bilateral relationship. Moreover, the rise of both countries as major powers has provided them with new tools and platforms to interact with each other, contributing to a spillover of the Sino–Indian relationship from the bilateral to regional level. Amid the rise of both countries as major trading and resource-consuming powers, this spillover effect or "nested security dilemma" is most evident in the maritime domain.[4] The fact that China and India are "hybrid powers"—that is, both are established continental and emerging maritime powers—adds to the complexity of their relationship and creates the potential for "horizontal escalation" as tensions along their disputed land border spill over into the maritime domain.[5] After charting the evolution of the Sino–Indian relationship, this article will focus on the potential for a nested security dilemma in the maritime domain. It also examines the implications of the changing nature of the Sino–Indian relationship on Asia's expanding strategic geography and US policy making toward Asia.

The Evolving Sino–Indian Relationship

The Sino–Indian relationship cannot be viewed as purely competitive or cooperative. The competitive dynamic in the bilateral relationship has been somewhat tempered by semi-institutional ties, such as the "India-China Strategic and Cooperative Partnership for Peace and Prosperity" that was concluded in 2005, the Strategic Economic Dialogue that began in 2011, and the conclusion of a Border Defense Cooperation Agreement in October 2013.[6] This complements earlier confidence-building measures reached in 1993 and 1996.[7]

Both countries' expanding military capabilities have also served to deter the outbreak of an all-out war, though this has also fueled the proclivity for limited stand-offs along their contested border. While lagging

behind China, India's fast-developing nuclear capabilities, including the expanded range of its ballistic missiles and development of a nuclear triad (confirmed by the launch of India's first indigenous nuclear submarine, the *Arihant* in 2009) has led to the presence of a credible nuclear deterrent in the Sino–Indian relationship.[8]

Growing economic interdependence has also served to deter open conflict between the two countries. China has emerged as India's leading trading partner, while India is China's leading trading partner in South Asia.[9] A plethora of deals were concluded during Chinese president Xi Jinping's visit to India in September 2014 and Indian prime minister Narendra Modi's visit to China in May 2015, including a five-year economic and trade development plan that entails the development of industrial parks and upgrading of India's rail network.[10] Xi also pledged to grant Indian companies, particularly those in the pharmaceutical, agricultural, and IT sectors—where India maintains a comparative advantage—greater access to Chinese markets to correct the long-standing imbalance in the trade relationship.[11]

However, contrary to rhetorical claims of Indian services complementing Chinese manufacturing and Chinese hardware complementing Indian software, there are limits to the level of economic interdependence between both economies.[12] An underlying disparity in the economic relationship has fueled this situation. Notably, India's exports to China are primarily natural resources, whereas China's exports to India are primarily manufactured and value-added products.[13] While bilateral trade has grown rapidly, crossing US $70 billion in 2014, it actually experienced a decline over the previous two years, while India's trade deficit with China has expanded to over $48 billion—amounting to almost 3 percent of India's gross domestic product.[14] Underlying mistrust in the bilateral relationship has also led to a poor investment relationship, with Chinese investment in India totaling a mere $400 million between 2000 and 2014—a fraction of China's total overseas investment.[15] This has been fueled by the persistence of non-tariff barriers, including India's national security establishment opposing Chinese investment in strategically important sectors such as ports and telecommunications and the introduction of mandatory local manufacturing rules.[16] India also remains one of the leading initiators of antidumping investigations against China, with the country imposing antidumping duties on 159

Chinese products between 1992 and 2013.[17] This has contributed to India's reluctance to grant "market economy" status to China.[18]

At the international level, both countries have cooperated on several issues of global governance through such forums as the Russia-China-India strategic dialogue and the Shanghai Cooperation Organization, where they have pledged to combat the threat of terrorism and called for the emergence of a "multi-polar world order".[19] Meanwhile, the G20 and BRICS (Brazil-Russia-India-China-South Africa) forums have emerged as key platforms for India and China to deepen regional economic integration, as evidenced by recent agreements for settling intra-BRICS trade in their local currencies and establishment of a BRICS New Development Bank and Asian Infrastructure Investment Bank.[20] The BASIC group of countries (comprising Brazil, South Africa, India, and China) has also emerged as a platform for cooperation on international climate-change negotiations.[21]

However, despite rhetoric of an emerging "Himalayan Consensus," there are clear limits to bilateral cooperation on global governance issues.[22] For instance, the December 2014 agreement between the United States and China on carbon emission–reduction targets for 2030 contrasts with India's reluctance to secure a similar agreement with the United States.[23] Notwithstanding the Joint Statement on Climate Change that was concluded between China and India in May 2015, there is a growing divergence between China and India on climate policies, with India maintaining a proclivity for a nonbinding approach with common but differentiated responsibilities, climate adaption over mitigation measures, and an emphasis on technology transfer and clean-energy financing.[24] The fact that both countries are at different stages of development has prompted this divergence of climate policies. India's per capita energy consumption remains among the lowest in the world; despite being the fifth-largest consumer of fossil fuels, India's per capita energy consumption is five percent that of the United States and 27 percent of China's per capita consumption.[25] However, China's per capita energy consumption is likely to plateau as its economy moves away from energy-intensive manufacturing, while there is still significant room for growth in India's energy consumption as it has yet to reach the full potential of its industrial capacity.

Even on regional issues where China and India potentially see eye-to-eye, both countries' differing diplomatic approaches act as barriers to

substantive cooperation. For instance, China and India maintain a joint concern over the destabilization of Afghanistan following the drawdown of Western forces, as both nations face the threat of terrorism emanating from Islamic extremism in Central and South Asia. These concerns have been evidenced by the establishment of a bilateral counterterrorism dialogue and joint exercises between their special forces.[26] Both countries have also made modest contributions toward strengthening the Afghan National Security Forces as part of protecting their growing economic interests in Afghanistan. This comes amid both countries' broader "pivot" toward the region under the aegis of China's "Silk Road Economic Belt" and India's "Connect Central Asia" strategy.[27]

Still, bilateral cooperation on stabilizing Afghanistan remains unlikely as long as both countries maintain a mismatch of vantage points. Notably, China continues to cling to its "all-weather" relationship with Pakistan, while India regards Pakistan as the root of Islamic extremist activity in the region. Moreover, China and India maintain a fundamentally different view of the role of the Afghan Taliban in the future of Afghanistan, with China playing a nascent mediating role and India continuing to regard the Taliban as a threat to stability.[28]

Border Troubles

At the root of mutual mistrust is the unresolved border dispute, which remains a thorn in the bilateral relationship. While China has resolved some 17 of 23 territorial disputes since 1949, limited progress has been made in the dispute with India under the special representatives' framework, which has been in place since 2003. The Line of Actual Control (LAC), distinguishing the disputed Indian and Chinese sides of the border, remains undemarcated—with no mutual agreement on the exact alignments of the border.[29] The fact that the LAC is today a matter of perception increases the potential for inadvertent conflict. Moreover, despite a few conciliatory gestures, such as opening border trade along the Nathu La, Lipu-Lekh, and Shipki La passes, both sides appear to be hardening their positions along the border. This has contributed to a surge in transgressions along the three sectors of the Sino–Indian border: western (Ladakh), middle (Uttarakhand and Himachal Pradesh), and eastern (Sikkim and Arunachal Pradesh). Tensions in the Depsang

Valley of eastern Ladakh in April 2013 and more recently in the Chumur area of Ladakh in September 2014 indicated as much.[30]

The changing strategic significance of the territorial dispute for both countries has hijacked the relatively simple solution of recognizing the de facto borders, which would entail India retaining control of Arunachal Pradesh and China controlling Aksai Chin.[31] For China, this refers to renewed instability in ethnically Tibetan areas since 2008 and latent concerns in Beijing that the passing of the 14th Dalai Lama may pave the way for the rise of a new generation of more radical Tibetan leaders who will adopt less conciliatory positions toward the Chinese government.[32] This has prompted Beijing to reaffirm its sovereignty over the Tibet Autonomous Region while adopting a more stringent position over its claim to all of Arunachal Pradesh, including the symbolically important town of Tawang, which is home to the largest Tibetan monastery outside Lhasa.

There are also no signs of China softening its all-weather relationship with India's long-standing rival, Pakistan. If anything, China appears to have backtracked on its more nuanced approach toward the India–Pakistan relationship that was portrayed by Beijing's neutral stance during the Kargil conflict in 1999.[33] Chinese infrastructure projects in Gilgit-Baltistan (in Pakistan-occupied Kashmir) reportedly often supported by the presence of Chinese military personnel, indicate implicit Chinese acceptance of Pakistan's claim over the disputed territory of Kashmir.[34] This has been reaffirmed by the conclusion of an agreement in April 2015 to commence work on the China–Pakistan Economic Corridor, parts of which pass through Pakistan-occupied Kashmir.[35] Further evidence of China's increasingly hardline position on the territorial dispute includes the denial of visas and issuing stapled visas to residents and officials from the Indian states of Arunachal Pradesh and Jammu & Kashmir.[36]

China's more aggressive posture on the territorial dispute in recent years can be attributed to the balance of power tilting in China's favor, with its defense budget and economy now being almost four times that of India.[37] This has contributed to China's strengthened military capabilities, which in turn have granted Beijing greater confidence and leverage to push India to resolve the territorial dispute on Chinese terms. This stands in contrast to China's offers to resolve the territorial dispute on mutually acceptable terms during periods of greater parity in the Sino–

Indian relationship, which was the case until the mid-1980s. While India has sought to correct this imbalance with the development of a new mountain strike corps and upgrading infrastructure along the disputed border, the asymmetry of material capabilities is likely to grow in the immediate future as China continues to outpace India in the development of border infrastructure.[38]

An additional dimension to the territorial dispute is the issue of water flows. Given both countries' growing water shortages and their still significant agrarian economies, the water-sharing issue threatens to enflame border tensions. Most of India's river systems originate in China, and the lack of trust stemming from the border dispute has deterred transparency and cooperation between both countries on sharing information on hydrology, dam-construction plans, and water-diversion projects.[39]

Conflicting Signaling

The increasing complexity of the bilateral relationship is evidenced by the sometimes-contradictory signals that have been sent out by both governments. The emergence of strong and decisive leaders in both countries—Xi Jinping in China and Narendra Modi in India—sets the stage for a clash of increasingly assertive foreign policies.[40] Modi, who made several visits to China during his tenure as chief minister of the Indian state of Gujarat, has spoken of emulating the Chinese development model while attracting Chinese investment to upgrade India's infrastructure and manufacturing capacity.[41] This alludes to a more cooperative and interdependent relationship. New Delhi maintains an aversion to any overt attempt to bandwagon against China. The fact that Modi visited China before completing his first year in office indicates the priority that he places on India's relationship with China. However, Modi's appointment of hawkish officials such as Vijay Kumar Singh, a retired Indian Army four-star general, to the position of minister of state for the North East Region (bordering China) and Ajit Doval, a former Indian intelligence officer, as national security advisor and special representative on the India-China boundary negotiations, signals a more muscular foreign policy. This has already been evidenced by such gestures as Modi's invitation to the prime minister of the Tibetan government-in-exile, Lobsang Sangay, to Modi's inauguration in May 2014.[42]

China has sent similarly conflicting signals on its relationship with India. Beijing has pledged to improve its relationship with New Delhi through expanding Chinese investment.[43] This has been complemented by a plethora of high-level official exchanges: Li Keqiang made his first overseas visit as Chinese premier to India in May 2013; Chinese foreign minister Wang Yi visited India shortly after Modi's inauguration in June 2014; and President Xi made an official state visit in September 2014.[44] However, even as it extends a hand of friendship to India, China is also adopting an increasingly hardline position toward its southern neighbor. This has been most prominently demonstrated by the timing of the most recent border tensions, which coincided with periods of high-level diplomatic exchanges. For examples, the Depsang Valley incident in April 2013 came ahead of the visit of Premier Li, while the tensions in the Chumur area in September 2014 coincided with the visit of President Xi.[45] Under previous administrations this may have been attributed to factionalism within the Chinese government arising from a more collective style of leadership.[46] However, under Xi's more centralized leadership this explanation seems less credible.[47] Xi's ongoing anticorruption campaign, which has entailed the purge of several senior-ranking military officials, may offer a possible explanation for the timing of these border transgressions as aggrieved groups within the People's Liberation Army (PLA) seek to embarrass the political leadership, as well as reaffirm the authority of the military on matters of national security.[48] Irrespective of whether these were coordinated actions or the result of frictions in civil-military relations, they serve to demonstrate China's proclivity for a carrot-and-stick approach toward India.

The propensity for misunderstanding is also fueled by limited people-to-people contacts, cultural barriers, and rising levels of nationalism that accompany the growing international clout of both countries.[49] This has been demonstrated by the jingoistic and alarmist media reporting in both countries, which has contributed to a climate of mistrust.[50] Both countries have sought to remedy this, as noted by the plethora of agreements concluded during Modi's visit to China, including the establishment of additional consulates, the introduction of an e-visa facility for Chinese nationals visiting India, and the establishment of a State/Provincial Leaders' Forum to facilitate interaction between local governments—in addition to stepping up cultural, education, media, and think-tank exchanges.[51] On a more fundamental level, neither

country has much experience in sharing power with the other. In the precolonial period, both civilizational states were essentially masters of their own domain, with a Himalayan divide separating them. However, the emergence of "disruptive technologies," such as ballistic missiles and cyber warfare, has reduced the strategic "space" between both states, thus, increasing the likelihood for misunderstanding and friction.

Finally, there is a fundamental mismatch of threat perceptions between both countries. Put simply, China is on India's radar, but India is not on China's radar to the same extent. While New Delhi focuses much of its foreign-policy attention and military resources on China, Beijing's primary strategic concerns are related to the US military presence in Asia and potential conflict in the Taiwan Strait, East and South China Seas, and the Korean Peninsula. The economic imbalance in the bilateral relationship has been a further catalyst for mutual misperception between both countries. At present, the Chinese economy is almost three times the size of the Indian economy in terms of purchasing power.[52] Whether the slowing Chinese economy and India's demographic dividend will alleviate this imbalance remains to be seen.[53]

Spillover in the Sino–Indian Relationship

Adding to their unresolved core grievances and conflicted signaling is the emergence of new theaters of interaction between both countries amid their rise as major powers with growing ambitions and capabilities. The joint statement concluded between China and India during Prime Minister Modi's visit to China in May 2015 acknowledged this growing potential for spillover in the bilateral relationship, noting that "as two major powers in the emerging world order, engagement between India and China transcends the bilateral dimension and has a significant bearing on regional, multilateral and global issues."[54] A notable example of this is the increasingly prominent role of third parties in the bilateral relationship—notably China's longstanding all-weather relationship with Pakistan and India's more recent rapprochement with the United States. As British historian Geoffrey Till notes, "neither China nor India see each other as their primary antagonist but do note that they are allied to the countries that are—the US and Pakistan respectively."[55] This has been supplemented by India's deepening relationships with Vietnam and Japan—China's traditional regional adversaries—and China's deepening relations with states of the Indian Ocean region. The fact that Modi's

visit to China in May 2015 was accompanied by a visit to South Korea and Mongolia and followed Xi's visit to Pakistan in April illustrates the growing presence of both countries along each other's peripheries.[56] This is further evidenced by the fact that Xi's visit to India in September 2014 was accompanied by visits to Sri Lanka and Maldives and preceded by Modi's visit to Japan and a visit by Indian president Pranab Mukherjee to Vietnam.

All of this demonstrates the potential for both India and China to leverage relations with third parties to influence their bilateral relationship. Modi's speech at Tsinghua University in May 2015 alluded to this by noting the need to "ensure that our relationships with other countries do not become a source of concern for each other."[57] India's sense of encirclement is reinforced by the fact that almost 70 percent of China's arms exports in 2010–14 went to Pakistan, Bangladesh, and Burma—countries along India's periphery.[58] This includes an "in-principle" deal for the sale of eight Chinese submarines to Pakistan, making it China's most expensive arms export deal to date.[59] Meanwhile, the first trilateral meeting of the foreign ministries of India, Japan, and Australia in June 2015 set the stage for a deepening strategic relationship among these three countries—to the quiet consternation of Beijing.[60] This comes within the broader context of China's recently unveiled "One Road, One Belt" concept and India's "Act East" policy, which have facilitated an expansion of both countries' extended neighborhoods.

Another example of the spillover of the bilateral relationship to the regional level is each country's growing voice in regional and global forums. In 2009 China attempted to block an Asian Development Bank loan to India, as the loan included funds for the Indian state of Arunachal Pradesh, which China claims as South Tibet.[61] The growth of regional and global forums where both countries have a prominent voice, including the BRICS New Development Bank, Asian Infrastructure Investment Bank, and Shanghai Cooperation Organization, could see the emergence of new theaters for cooperation but also potential proxy wars in the bilateral relationship.

Nested Security Dilemma in the Maritime Domain

This spillover effect is captured in the concept of a nested security dilemma.[62] The concept of a *nested security dilemma* is based on the idea that security dilemmas involving major states have externalities beyond

their bilateral relationship, with implications for regional and global security.[63] Employing the concept of a nested security dilemma as an explanatory tool demonstrates how China's and India's responses to each other's actions can have impacts beyond their bilateral relationship, with implications for the wider regional security dynamic.

Expanding Maritime Interests and Capabilities

Further evidence of this nested security dilemma in the Sino–Indian relationship is the emergence of Asia's maritime domain as a platform for interaction and potential competition between both states. China and India have historically been viewed as continental powers, with land-based forces traditionally dominating their militaries while navies have played a secondary role in forging their military doctrines and strategies. Both countries have usually pursued relatively modest naval strategies confined to playing a supporting role to land-based operations and protecting their respective coastlines. China's focus has been on sea-denial capabilities aimed at deterring US intervention in a conflict in the Taiwan Strait, while India has focused on coastal defense and surveillance, given the country's porous, poorly demarcated and disputed maritime border.

However, the rise of China and India as major trading and resource-consuming powers has elevated the strategic importance of the maritime domain. The numbers speak for themselves. More than 90 percent of India's total external trade by volume and 77 percent by value now transits the maritime domain.[64] This includes more than 70 percent of the country's oil imports.[65] Meanwhile, more than 90 percent of China's foreign trade by volume and 65 percent by value are seaborne, including 85 percent of its oil imports.[66] Both countries' expanding maritime interests are also manifested in the emergence of more assertive naval doctrines and the growth of historical narratives that reaffirm the importance of their maritime traditions. In China, growing dependence on imported resources has fueled concerns over a so-called "Malacca Dilemma," which refers to strategic vulnerabilities rooted in China's dependence on resources imported through sea lanes patrolled by potentially adversarial countries.[67] This has prompted the country's maritime strategy to move beyond its traditional focus on "near-coast defense" toward "near-seas active defense" and increasingly into the realm of "far-sea operations"—or what China's latest defense white paper termed as "open

seas protection."[68] China's maritime ambitions have been reflected in its 2013 defense white paper, noting the need to "develop blue water capabilities" and the introduction of "new historic missions" in 2004, which served to redefine China's national defense strategy to include new geographic and functional areas. These statements demonstrate a growing consensus that "over the long-term, Beijing aspires to sustain naval missions far from China's shores," according to a recent report by the US Office of Naval Intelligence.[69] Meanwhile, India has declared ambitions to develop "a brand new multi-dimensional Navy" with "reach and sustainability" extending "from the north of the Arabian Sea to the South China Sea."[70] Renewed Chinese attention on the naval voyages of Zheng He during the Ming dynasty in the fifteenth century and in India on the naval expeditions of the Chola dynasty during the eleventh century has also demonstrated a concerted effort by both states to elevate the strategic importance of their naval traditions.[71] The views of proponents of expanding naval power, such as the late Chinese admiral Liu Huaqing and the late Indian historian K. M. Panikkar, have also found renewed support during the current maritime renaissance in both states.[72]

Operationalizing these growing naval ambitions and interests, both countries have rapidly developed their maritime capabilities. China has established a fourth fleet on the southern island of Hainan. This fleet, which will complement the North Sea Fleet based in Qingdao, East Sea Fleet in Ningbo, and South Sea Fleet based in Zhanjiang, demonstrates China's growing maritime interests in the South China Sea, Indian Ocean, and beyond.[73] These expanded capabilities have been revealed in demonstrations of China's projection of naval power beyond its traditional sphere of interest around the first and second "island chains."[74] These include the PLA Navy's (PLAN) South Sea Fleet deploying a task group for its first training exercise in the eastern Indian Ocean in 2014, a month-long visit of two Chinese missile frigates to the Mediterranean Sea and eastern Atlantic in 2013, as well as deployment of three PLAN vessels to South America the same year, which followed the PLAN's first naval exercises in the Pacific Ocean in 2011 and its revolving ship deployment in support of antipiracy operations in the Indian Ocean since 2009.[75] More recently, the Chinese and Russian navies conducted joint naval exercises in the eastern Mediterranean in May 2015.[76]

Meanwhile, India's tri-services Andaman and Nicobar (Southern) Command, which was established in 2001, has been referred to as India's

"window into East and Southeast Asia."[77] This has complemented the Eastern Command headquartered in Visakhapatnam, Andhra Pradesh, and a new facility codenamed "Project Varsha" under development near the coastal town of Rambilli, Andhra Pradesh. On the western coast, Indian Naval Station Kadamba in Karwar, Karnataka, aims to protect maritime trade routes in the Arabian Sea, while alleviating pressure on the Western Command in Mumbai.[78]

Both countries also have ambitious plans for the development and acquisition of platforms aimed at strengthening their blue-water naval capabilities. China currently maintains a fleet of 300 surface combatants, submarines, amphibious ships, and patrol aircraft, with more than 60 vessels laid down, launched, or commissioned in 2014 alone. Moreover, its procurement of naval platforms has become increasingly indigenous, with its last import of a major naval platform taking place in 2006.[79] Meanwhile, India has ambitions to develop a 160-plus-ship navy by 2022, with more than 40 warships and submarines on order or under construction at the country's three major shipyards.[80] Moreover, the fact that China and India are two of only three Asian countries and two of only 10 countries in the world to maintain aircraft carriers illustrates their ambition to project power beyond their immediate subregions. Despite the hype surrounding the launch of China's first aircraft carrier, the *Liaoning*, which was commissioned in 2012, the fact that China is in the process of developing two more indigenously-developed carriers (with ambitions for 4–6 carriers) is indicative of the trajectory that Beijing sees for itself in the maritime domain.[81] As military analyst Richard Bitzinger notes, "One aircraft carrier may be symbolic, but four to six carriers is a new maritime strategy."[82] Similarly, India has a target to develop three aircraft-carrier battle groups by 2022, which was confirmed by the unveiling of the country's first indigenously developed carrier, the INS *Vikrant* in 2013, and plans for the development of the larger INS *Vishal* as part of the indigenous aircraft carrier-II project.[83] To be sure, China remains a long way from developing the necessary capabilities—including training, doctrine, and support vessels—to successfully operate a carrier battle group.[84] This comes as aircraft carriers are exposed to growing vulnerabilities amid the proliferation of sea-denial platforms such as submarines, antiship ballistic missiles, and improved surveillance platforms. Nonetheless, any state seeking to project power and exercise sea-control will require carrier-group capability.

Similarly, while some 36 countries maintain submarines in their navies, China and India are two of only six countries with a nuclear-submarine capability. China has recently unveiled its most advanced Type-093G *Shang*-class nuclear-powered attack submarine (SSBN), with the quantity of China's conventional and nuclear submarine fleet now surpassing the United States—though it does not yet match the United States in the quality of its vessels.[85] Meanwhile, India's first indigenously built SSBN, the INS *Arihant*, is undergoing sea trials, while the first of the country's indigenously built diesel-electric *Scorpene*-class submarine was launched in April 2015.[86] Both countries' interests in moving beyond their predominantly diesel submarine fleet toward building up their nuclear submarine capability point toward a growing interest in power projection beyond their littoral regions. Both countries' development of multimission platforms, such as China's *Luyang III*-class destroyers and *Jiangdao*-class corvettes and India's acquisition of the INS *Jalashwa* (formerly the USS *Trenton*), a landing platform dock ship acquired from the United States in 2007, also points to a growing interest in power projection.[87]

Clash of Interests

Applying the concept of the nested security dilemma, the rise of China and India as major maritime powers has implications beyond the confines of their bilateral relationship, fueling the potential for both competition and cooperation. On the one hand, discourse of Sino–Indian naval competition has become increasingly common in recent years. Naval analyst Toshi Yoshihara notes for instance that "as New Delhi and Beijing look seaward, both powers will jostle for influence and advantage across the entire Indo-Pacific maritime theatre."[88] Indian strategic thinker Raja Mohan adds that the "growth of [China's and India's] naval capabilities and the broadening of their maritime horizons in recent years will extend the security dilemma—which has expressed itself until now in the land of inner Asia—to the waters of the Indian and Pacific Oceans." In doing so, the bilateral relationship between the two Asian powers has "begun to generate a competitive dynamic enveloping the entire Indo-Pacific littoral."[89] George Perkovich echoes this position by noting the emergence of a "swelling Sino–Indian security dilemma into the Indian and Pacific oceans" amid both countries' growing ability to "build capacity to project power and secure their lines of communica-

tion in increasingly distant waters (so that), China will seem to encroach on India's sphere of influence in the Bay of Bengal and Indian Ocean, while India will seem misplaced in the South China Sea and the Strait of Malacca."[90]

Echoing these assessments, naval discourse in both countries increasingly reflects Mahanian thinking, with an emphasis on sea-control and competitive naval diplomacy, while moving away from a traditionally defensive maritime posture. Foreign policy analyst Raja Mohan notes that "as New Delhi and Beijing define their maritime approaches in terms of the US Monroe Doctrine, the two would seem bound to step on each other's toes."[91] Notably, China's increasingly assertive position over territorial disputes in the South and East China Seas has been viewed by some as a harbinger of its potential behavior in the Indian Ocean. This will be the case if China elevates the protection of sea-lines of communication to a "core interest" (*hexin liyi*) on par with its security and sovereignty interests of reclaiming "lost territories." India's maritime doctrine has been even more explicit, stating that "sea control is the central concept around which the Indian navy is structured."[92]

This competitive dynamic is already evident with China and India challenging each other in their respective littoral spaces in the Indian Ocean and South China Sea. For instance, India has echoed the US position on maritime territorial disputes in the East and South China Seas by calling for their peaceful resolution and maintaining the freedom of navigation.[93] This has become more emphatic under the Modi government, as noted by the joint statement issued following the visit by Pres. Barack Obama to India in January 2015 that made specific reference to "safeguarding maritime security and ensuring freedom of navigation and over flight throughout the region, especially in the South China Sea."[94] This was the first time both countries made such an explicit reference to the territorial dispute in a bilateral context. Moreover, India has injected itself into the disputes through its pursuit of deepening relations with several claimant states. For instance, India and Japan held their first bilateral naval exercises in June 2012.[95] India has also agreed to equip Vietnam with naval patrol boats, as well as providing training to the country in underwater warfare, while having discussions to supply Vietnam with India's BrahMos supersonic cruise missile.[96]

This has come to the chagrin of China, which maintains a preference for a bilateral, non-internationalized approach in resolving these dis-

putes. Reports in July 2011 that an Indian navy vessel, the INS *Airavat*, received alleged radio contact from the Chinese navy demanding that the vessel depart disputed waters in the South China Sea after completing a port call in Vietnam illustrate China's opposition to an expanding Indian naval presence in East Asia.[97] This was followed by the less belligerent but nonetheless provocative gesture of an Indian naval vessel, INS *Shivalik*, receiving a PLAN escort while on its way from the Philippines to South Korea in June 2012.[98] Beijing has also opposed Vietnam granting exploration rights in offshore blocks located in disputed waters to Indian company ONGC Videsh.[99]

Meanwhile, India has voiced concerns over China's growing presence in the Indian Ocean under the aegis of its Maritime Silk Road (MSR) concept.[100] Unveiled by President Xi in 2013 during a tour of Southeast Asia, the MSR has now extended to the Indian Ocean region, with endorsements from several countries in the region.[101] As well as securing maritime trade routes, China's interests in the Indian Ocean are also rooted in the country's deep-sea mining concessions in the southern Indian Ocean.[102] This has led to the emergence of a latent Sino–Indian rivalry in the Indian Ocean, which was evidenced by reports that an Indian attack submarine and Chinese naval unit were "locked in a tense stand-off" near the Bab-el-Mandeb Strait in the Gulf of Aden in January 2009.[103] More recently, a Chinese nuclear attack submarine made its first declared operational deployment into the Indian Ocean in February 2014, while a *Song*-class diesel-electric submarine docked at a Sri Lankan port in September 2014.[104] As international affairs scholar John Garver notes, "by slowly expanding its naval presence in the Indian Ocean, Beijing is trying to create a new status quo."[105] In response to these developments, India has strengthened its antisubmarine capabilities, as demonstrated by the launch of the indigenously built INS *Kamorta* guided-missile destroyer in August 2014.[106]

Moreover, the Sino–Indian maritime rivalry is increasingly moving onshore, as manifested by the development of transshipment hubs along maritime trade routes. This "String of Pearls" strategy, which China has sought to rebrand as the more benign MSR, is evidenced by the development of ports along maritime trade routes, including Gwadar in Pakistan and Hambantota in Sri Lanka.[107] As the PLAN has stepped up port calls in the region, there have been calls by some in China to establish a "long-term supply base" near the Gulf of Aden, with some 18 possible

sites reportedly under consideration to establish "overseas strategic support bases" in the Indian Ocean region.[108]

India has countered China's String of Pearls with its own so-called "Necklace of Diamonds."[109] This is noted by the Indian navy gaining permanent berthing rights at Vietnam's Na Thrang port, which has confirmed New Delhi's ability to extend its "sustainable maritime presence" into the South China Sea.[110] India's establishment of a monitoring station in Madagascar complements plans for a similar facility in Mauritius and established berthing rights in Oman, which are expanding the Indian Navy's permanent presence in the southern Indian Ocean. While claims that these port facilities have a military role are exaggerated at present, it is not inconceivable that both countries could eventually use these commercial ports for multiple purposes, including resupply, refueling, and even surveillance and signals intelligence. However, given their historical aversion to overseas bases, it is more likely that both countries will pursue a strategy of "places, not bases" with arrangements to gain privileged access to overseas facilities rather than establishing permanent overseas bases.[111] In this context, both countries have sought to court island states in the Indian Ocean region, including Maldives, Mauritius, Seychelles, and Sri Lanka, as part of a long-term maritime strategy to secure exclusive security partnerships with states strategically located along important sea-lines of communication.[112] Notably, the decision in February 2015 by the Sri Lankan government to review the terms of Chinese investment in a port city project in Colombo, Sri Lanka, alludes to the nascent Sino–Indian rivalry for privileged access to port facilities in the Indian Ocean region.[113]

Convergence of Interests

At the same time, the security dynamic in the maritime domain has not been purely competitive, as evidenced by the recent establishment of a bilateral maritime security dialogue between China and India.[114] Both countries have also coordinated their antipiracy patrols in the Indian Ocean within the framework of the Shared Awareness and Deconfliction mechanism. As former Indian national security advisor Shivshankar Menon notes, "over the last decade an Indian presence in the waters east of Malacca and a Chinese presence west of Malacca have become the new norm. Both have happened simultaneously and without apparent friction."[115]

Both countries have the potential to play a stabilizing and constructive role in the maritime domain. For instance, humanitarian assistance/disaster relief (HADR) operations have served to enhance the Indian navy's reputation, as noted by its participation in relief operations following the Asian tsunami of 2004 and the cyclone that struck Burma in 2008.[116] The Indian navy also escorted US naval vessels transiting the Strait of Malacca as part of Operation Enduring Freedom in 2002.[117] In the five years since October 2008, when India began supporting antipiracy operations in the Gulf of Aden, the Indian navy has escorted over 1,100 vessels through the Internationally Recommended Transit Corridor, as well as reportedly capturing 100 pirates and foiling more than 40 piracy attempts.[118] India has also been successful at regional confidence building in the maritime domain, fueled by the growing frequency of joint naval exercises with regional navies. This includes the biennial Milan (that involves 15 countries since 1995); the search and rescue operations, with Malaysia, Singapore, and Indonesia since 1997; and Malabar exercises with the United States (and intermittent participation of Japan since 2007). This has supplemented joint bilateral naval exercises with several countries ranging from Singapore (since 1993) to Japan (beginning in 2013) and coordinated patrols with several countries, including Indonesia (since 2002) and Thailand (since 2005). The momentum of these interactions has increased since Prime Minister Modi announced his Act East policy in 2014.[119] The Indian navy has since stepped up port calls in East Asia and Oceania, including announcing the first bilateral naval exercises with Australia.[120]

While India has so far taken the lead on regional confidence-building, China's rhetoric of maintaining "harmonious seas" and engaging in military operations other than war suggest that its proclivity for cooperation in the maritime domain could grow as its maritime interests move further from its coastline.[121] This is illustrated by the case of the country's antipiracy operations in the Indian Ocean, where the PLAN has escorted more than 6,000 Chinese and non-Chinese vessels, including UN World Food Program convoys.[122] Such operations are likely to become increasingly commonplace given the growing outbound investment by Chinese companies, much of which is in countries with unstable regimes. The induction of one of the world's largest hospital ships, the *Peace Ark* in 2008, which was deployed for its first disaster relief mission in 2013 following a typhoon in the Philippines, is further

evidence of the Chinese navy's growing humanitarian response capabilities.[123] China's participation in the 2014 Rim of the Pacific exercise in Hawaii is further evidence of the potential for confidence-building and cooperation in the maritime domain.[124]

Ultimately, India and China have a shared interest in maintaining open sea lanes, given the strategic importance of major waterways as transit points for growing trade and resource imports and combatting the scourge of nontraditional security threats—including maritime piracy, terrorism, and arms, narcotics, and people trafficking. In this context, Indian diplomat Shivshankar Menon has proposed the creation of a "Maritime Concert" in which the region's major maritime powers would have collective responsibility to protect the Indian Ocean.[125]

China and India as Hybrid Powers

Complicating the nested security dilemma in the Sino–Indian maritime relationship is the fact that China and India are hybrid powers, meaning they are countries that are both major continental and emerging maritime powers.[126] In other words, China's and India's ongoing naval transformations challenge the notion that a state's status as a continental or maritime power is permanent, static, or mutually exclusive. The most notable evidence of this is China's near simultaneous unveiling of the dual concepts of a "Silk Road Economic Belt" and "21st Century Maritime Silk Road," which have been integrated into the One Belt, One Road initiatives. These concepts promote greater infrastructure connectivity, economic integration, and strategic cooperation across China's land and maritime frontiers, respectively.[127] This reflects the broader regional context in Asia in which sea power and land power are emerging as "an interactive dyad" amid the continued strategic relevance of continental Asia, despite the growing strategic importance of maritime Asia.[128]

This interactive dyad between sea and land power creates the potential for horizontal escalation in the Sino–Indian relationship, with tensions along their disputed land border leading to potential frictions in the maritime domain.[129] As one Indian strategic analyst notes, "if pushed to the wall or confronting coercion on the Himalayan frontiers, India can use an asymmetric maritime option by targeting China's vulnerability in the IOR [Indian Ocean region]."[130] Thus, resolving the nested security

dilemma in the Sino–Indian maritime relationship will require transcending the maritime domain and addressing the root causes of mutual mistrust. As Geoffrey Till notes, "naval relations between the two countries [China and India] are largely set by continental concerns."[131] This implies that maritime confidence building will require addressing unresolved core grievances in the bilateral relationship, namely the long-standing territorial dispute along the shared Himalayan border.

Expanding Asia's Strategic Geography

Examining the broader implications of the nested security dilemma in the Sino–Indian maritime relationship, the rise of China and India as major trading and resource-consuming powers and their concomitant ability to project power beyond their immediate subregions has widened the strategic geography of Asia. The very emergence of Indo–Asia Pacific, or the Indo-Pacific in its abbreviated form, as a new geopolitical space is a reflection of China's and India's abilities to transcend their respective subregions. As former Australian minister for defence Stephen Smith notes, "so significant is India's rise that the notion of the Indo-Pacific as a substantial strategic concept is starting to gain traction."[132] International strategist Rory Medcalf also notes that China is the "quintessential Indo–Pacific power," given that it is the "expansion of China's interest, diplomacy and strategic reach into the Indian Ocean that most of all defines the Indo–Pacific."[133]

Looking ahead, while the Indian Ocean and South China Sea remain the most likely theaters of a nested security dilemma in the Sino–Indian maritime relationship, it is conceivable to envision new theaters of interaction between both countries. Notably, the emergence of China and India as major maritime powers coincides with both countries' growing interests in the Middle East. The Middle East, or West Asia, now accounts for 50 percent of China's oil imports and 70 percent of India's oil imports.[134] More broadly, this reflects Asia's growing resource interdependence with the Middle East. Asia buys 75 percent of the Middle East's oil exports, which account for half of Asia's oil consumption.[135] With the Middle East being home to 65 percent of the world's proven oil reserves and 45 percent of its natural gas, the symbiotic relationship between East and South Asia as major sources of oil demand and the Middle East as the preeminent oil supplier is set to grow.[136] Ironically,

while the United States has proclaimed its "pivot" or "rebalance" toward Asia, Asia is simultaneously pivoting toward the Middle East amid both regions' growing resource interdependence.[137]

This increasingly symbiotic relationship between the Middle East and Asia extends to the security arena, given the need for stability in energy-supplier states and along energy-transit corridors. In this context, prolonged instabilities in the Middle East amid the ongoing Arab uprisings and civil wars in Iraq and Syria, a blockade along the Strait of Hormuz due to conflict with Iran, or disruptions along the Gulf of Aden due to piracy, or terrorism emanating from the Horn of Africa pose growing strategic risks for China, India, and other major oil importing Asian powers. As energy researcher John Mitchell notes, "Asia is more at risk from disruption of Middle East oil supplies than is either Europe or the United States, yet as a whole it is less prepared to deal with such an upheaval."[138] China and India are even more vulnerable in this context, given their lack of sizable reserve capacity that would insulate them from supply-side shocks in the event of instabilities in the Middle East.[139] India's vulnerability is further exacerbated by the fact that almost 80 percent of its crude imports come through the Strait of Hormuz—compared to just more than 20 percent for China.[140]

Furthermore, China's and India's interests in the Middle East are not confined to hydrocarbons. Some 40 percent of China's exports go to the Middle East and North Africa, while more than half of India's foreign remittances emanate from this region.[141] India also maintains a sizable diaspora of more than 6 million people in the Persian Gulf states. China's and India's interlinkages with the Middle East extend to the domains of bilateral investment in hydrocarbon storage and refining capacity and nonhydrocarbon projects, such as joint ventures in developing renewables and nuclear power, construction and labor contracts, aid, grants, and sovereign wealth funds.[142]

At present, China's and India's economic interactions with the Middle East far exceed their strategic engagement with the region. Both countries remain free riders of the regional security order that has been largely enforced by the United States in the post–Cold War period. However, there are signs of change amid both countries' strategic dialogue with the Gulf Cooperation Council, China's appointment of a special envoy for the Middle East in 2002, the establishment of the China–Arab Cooperation Forum in 2004, the launch of India's "Look West" policy in

2005, and China's appointment of an envoy for the Syrian conflict in 2012.[143] Both countries have stepped up military-to-military engagement with the region, including with regional navies. India has held annual naval exercises with Oman since 1993; joint naval exercises with Iran in 2003 and 2006; a large-scale Theatre Readiness Operational exercise (Tropex) involving vessels of its Western and Eastern Commands in the Arabian Sea in 2007; as well as exercises with the navies of Kuwait, Bahrain, Saudi Arabia, and the United Arab Emirates.[144] The Indian Ocean Naval Symposium, which was established in 2008, has provided another avenue for India's interaction with navies of the Persian Gulf. China's strategic engagement with the region began with arms transfers to the region, including the sale of CSS-2 missiles to Saudi Arabia and Silkworm missiles to Iran.[145] While the United States remains a key supplier of military hardware to the region, China has expanded its role as evidenced by the sale of DF-21 ballistic missiles to Saudi Arabia and the HQ-9 long-range surface-to-air system to Turkey.[146] China has also participated in the biennial Aman naval exercises with Pakistan in the Arabian Sea since 2007, while making port calls in Cairo, Haifa, and Istanbul in 2012 and holding its first joint naval exercises with Iran in September 2014.[147] The same year, a Chinese frigate was deployed to escort an international convoy that removed Syria's chemical weapons stockpile.[148]

Amid China's and India's growing investments in the Middle East and the plethora of instabilities plaguing the region, both countries have also had to strengthen their humanitarian response and expeditionary capabilities. For instance, the Indian navy was used to evacuate its nationals from the civil war in Libya in 2011 and Indian, Sri Lankan, and Nepalese nationals from the conflict in Lebanon in 2006.[149] Meanwhile, a Chinese missile frigate was deployed to the Mediterranean Sea in early 2011 to support the evacuation of more than 38,000 Chinese nationals from Libya.[150] The instabilities in Yemen have provided the most recent example of the growing HADR capabilities of both countries in the region. In addition to evacuating over 4,500 of its own nationals, India was involved in rescuing civilians from 41 nations.[151] Also, the PLAN evacuated more than 600 of its nationals, as well as civilians from 15 other countries in Yemen.[152] Renewed instabilities in Iraq will further test China and India, given their sizable interests in the country. These

include the presence of some 10,000 Chinese nationals in Iraq and China's position as a leading buyer of Iraqi oil.[153]

Looking ahead, the Sino–Indian maritime relationship in the South China Sea and Indian Ocean offers a potential indicator of how the bilateral relationship could play out in the Middle East. In this context, a more complex dynamic could emerge in the region as the unipolar external presence of the United States gives way to a more multipolar orientation in which the Sino–Indian relationship serves to overlay preexisting fissures in the region. However, an alternative outlook for the Sino–Indian relationship is evidenced by the fact that China and India have often shared overlapping perspectives on developments in the Middle East. This is evidenced by both countries' historically close relations with countries that the United States has labelled pariah regimes, including Iran, Syria, and Libya, as well as China's and India's concerns regarding the Arab uprisings and opposition to Western military intervention in Libya and Iraq. This leads to the potential for a greater convergence of interests between both countries in the Middle East. However, this also alludes to a different dynamic between regional and extraterritorial powers, with a reversion to traditional Westphalian norms of interaction emphasizing sovereignty, territorial integrity, and nonintervention over humanitarian intervention and democratic regime change. Ultimately, China's and India's growing maritime interests and capabilities offer to both widen the strategic geography of Asia and change the nature of their bilateral relationship.

Implications for US Policy toward Asia

The evolving Sino–Indian relationship also has implications for the US policy toward Asia. First, the United States has not been a bystander to the evolving Sino–Indian relationship. In many ways the spillover or nested security dilemma of the Sino–Indian relationship has been facilitated by the United States, as the country has actively sought to draw India deeper into the regional security architecture of East Asia. The plethora of statements by senior US officials in support of a stepped-up Indian role in the region is evidence of this. For instance, former Secretary of State Hillary Clinton has stated that the United States has "made it a strategic priority to support India's 'Look East' policy and encourage Delhi to play a larger role in Asian institutions and affairs."[154]

Ben Rhodes, deputy national security advisor, has noted that "just as the United States, as a Pacific Ocean power, is going to be deeply engaged in the future of East Asia, so should India as an Indian Ocean power and as an Asian nation."[155] President Obama has called on "India to 'engage East'," while the joint statement reached between India and the United States has noted a "shared vision for peace, stability and prosperity in Asia, the Indian Ocean region, and the Pacific region."[156] Former Secretary of Defense Leon Panetta has noted that "India is the lynchpin" of US strategy "in the arc extending from the Western Pacific and East Asia into the Indian Ocean region and South Asia."[157] Similarly, Deputy Secretary of State William Burns has noted, "India's strong presence across the Indian and Pacific Oceans is a source of comfort and affirms its potential as a net security provider in the maritime domain."[158]

Moreover, India–US strategic cooperation is being cemented by a shared perception of the rise of China as an emerging maritime power amid "a common Indo–Pacific maritime challenge emerging from the People's Republic of China to India in the Indian Ocean and to the United States in the Pacific Ocean."[159] International relations scholar David Scott adds that "US–India formal agreements and informal understanding are being constructed and carefully calibrated in the Indo-Pacific with China considerations very much in mind (and in deployment patterns), even if not in official speech."[160] International security specialist Ashley Tellis has also noted the linkage between China's growing maritime power-projection capabilities and India–US cooperation: "Beijing's recent appearance in the northern Indian Ocean has effectively unified the Indo-Pacific strategic space in a way that strengthens New Delhi and Washington's already converging interests."[161]

Furthermore, as the region's dominant military power and sea-based balancer, the United States has a crucial role to play in ensuring that the emergence of China and India as major maritime powers does not undermine the stability of the maritime global commons. As Mohan notes, "as the economic stakes of China and India in the oceans steadily expand and the two sides proceed with the building of powerful navies, a substantive and open-ended dialogue between the two security establishments on maritime and naval issues has become an urgent imperative."[162] In this context, while India and China have established a bilateral maritime security dialogue, this initiative remains largely consultative and lacks a rules-based structure.[163] A more robust initiative

could be an "incidents at sea agreement" between both countries, which would echo a similar agreement reached between the United States and the erstwhile Soviet Union in 1972 at the height of the Cold War in the Incidents on and over the High Seas agreement. This would facilitate information exchange, provide a mechanism to manage incidents, and ultimately strengthen mutual understanding. The United States could seek to facilitate this process.

Conclusion

Historically, the strategic weight of China and India in Asia has made their bilateral relationship a microcosm of broader regional dynamics and a harbinger of the regional architecture. During the colonial period, interaction between China and India was subordinated to colonial rivalries, as Indian opium and soldiers were used to gain markets and quash rebellions in China.[164] In the postcolonial period, initial cordiality in the Sino–Indian relationship was accompanied by Asian and developing-world solidarity through such initiatives as the 1947 Asian Relations Conference and the "Bandung spirit" of 1955, which became the precursor to the Non-Aligned Movement and Asia-Africa Summit. The Five Principles of Peaceful Coexistence, also known as the Panchsheel Agreement, not only served as a symbol of friendship between two of the world's most populous countries but also codified the process of interaction within the developing world and became an antecedent to subsequent norms of regional interaction, such as the Association of Southeast Asian Nations's Treaty of Amity and Cooperation.[165] Finally, growing animosity in the Sino–Indian relationship was accompanied by a fracturing of the regional architecture along the Cold War divide. As Menon notes, the 1962 Sino–Indian war "brought a sense of dismay to pan-Asian aspirations: if Asia's two largest nations were in discord, pan-Asian concord was a pipedream."[166]

This linkage between the nature of the Sino–Indian relationship and the regional order will continue to gain momentum in the post–Cold War period, as the rise of both countries as major regional and global powers with growing political, economic, and military weight in the international system makes their bilateral relationship more strategically significant. Moreover, the multidimensional nature of the Sino–Indian relationship has served to further amplify the significance and complex-

ity of the bilateral relationship. On one hand, border frictions, resource competition, and both countries' engagement with each other's strategic rivals will remain sources of mutual mistrust in the bilateral relationship. On the other hand, China is also an increasingly important economic partner for India and a potential ally on issues of global governance.

To be sure, in recent years the Sino–Indian relationship has been subordinated to increasingly pragmatic foreign-policy approaches by both countries. This is in stark contrast to their ideologically-driven foreign policy during the Cold War, which was embedded in India's Nehruvian nonalignment and China's Maoist vision of revolutionary world struggle. This newer approach will serve to temper any rash or aggressive foreign-policy actions. Instead, as both countries remain focused on growth, development, and consolidation of political power, any rivalry is likely to manifest itself in the realm of rhetoric, economics, military modernization, and competition for allies. Nonetheless, given their growing strategic weight in the international system, the relationship between these two emerging powers cannot be overlooked. The last major conflagration between the two coincided with (and was overshadowed by) the Cuban missile crisis. However, unlike their brief border war in 1962, future hostilities in the Sino–Indian relationship are likely to take center stage rather than being relegated to a mere sideshow. SSQ

Notes

1. The Five Principles of Peaceful Coexistence—also known as the Panchsheel Agreement/Treaty—refers to mutual respect for sovereignty and territorial integrity; mutual nonaggression; noninterference in each other's internal affairs; equality and mutual benefit; and peaceful coexistence.

2. For a detailed background of the 1962 Sino–Indian border war see: Srinath Raghavan, "The Disputed India–China Boundary 1948–1960" and "China, 1961–62," in *War and Peace in Modern India* (London: Palgrave Macmillan, 2010).

3. V. Natarajan, "The Sumdorong Chu Incident," *Bharat Rakshak Monitor* 3, no. 3 (November–December 2000), http://www.bharat-rakshak.com/MONITOR/ISSUE3-3/natarajan.html.

4. George J. Gilboy and Eric Heginbotham, *Chinese and Indian Strategic Behavior: Growing Power and Alarm* (New York: Cambridge University Press, 2012).

5. Luis Simon, "Reaching Beyond the Indo-Pacific," *Comparative Strategy* 32, no. 4 (2013), 337.

6. Border Defence Cooperation Agreement (BDCA) between India and China, *Indian Defence Review*, 23 October 2013, http://www.indiandefencereview.com/news/border-defence-cooperation-agreement-bdca-between-india-and-china/; and Jagannath P. Panda, "India-

China Strategic Economic Dialogue (SED): Progress and Prognosis," *IDSA Issue Brief*, 3 April 2014, http://www.idsa.in/issuebrief/IndiaChinaStrategicEconomicDialogue_jppanda_030414.html.

7. Swaran Singh, "Three Agreement and Five Principles between India and China," in *Across the Himalayan Gap*, ed. Tan Chung (New Delhi: Indira Gandhi National Centre for the Arts, 1998).

8. Rajaram Panda, "Arihant: Strengthening India's Naval Capability," *IPCS Issue Brief*, no. 115, September 2009, http://www.ipcs.org/issue-brief/navy/arihant-strengthening-indias-naval-capability-115.html; "India Sails toward N-sub Club," *China Daily*, 27 July 2009; and "India Ups Regional Nuclear Ante with New Sub," *South China Morning Post*, 30 July 2009.

9. Dilasha Seth, "India's Trade Deficit with China to Double in the Next Two Years," *Economic Times* (India), 6 April 2015, http://articles.economictimes.indiatimes.com/2015-04-06/news/60865975_1_india-s-trade-deficit-tariff-concessions.

10. Victor Mallet and Lucy Hornby, "India and China Sign $22bn in Deals during Modi Visit," *Financial Times*, 17 May 2015, http://www.ft.com/cms/s/0/88de2eea-fc60-11e4-ae31-00144feabdc0.html; and Press Trust of India, "China President Xi's India Visit: China Set to Pump Billions of dollars in India; Outwit Japan," *Economic Times* (India), 14 September 2014, http://articles.economictimes.indiatimes.com/2014-09-14/news/53904022_1_india-visit-prime-minister-narendra-modi-railway.

11. Amol Sharma, "Trade Gap Strains India-China Ties," *Wall Street Journal*, 3 August 2012, http://online.wsj.com/news/articles/SB10000872396390443687504577563542149677000.

12. "The Myth of Chindia," *Economist*, 22 November 2006, http://www.economist.com/node/8311987; Peter Engardio, ed., *Chindia: How India and China Are Revolutionizing Global Business* (New York: McGraw Hill, 2007); and Jairam Ramesh, *Making Sense of Chindia: Reflections on China and India* (New Delhi: India Research Press, 2005).

13. Seth, "India's Trade Deficit with China"; and Saibal Dasgupta, "India to Question China on Market Access, Balance of Trade," *Times of India*, 18 January 2010, http://timesofindia.indiatimes.com/india/India-to-question-China-on-market-access-balance-of-trade/articleshow/5474002.cms.

14. Reuters, "India to Seek End to Non-tariff Barriers during Narendra Modi's China Visit," *Economic Times* (India), 9 May 2015, http://economictimes.indiatimes.com/news/economy/foreign-trade/india-to-seek-end-to-non-tariff-barriers-during-narendra-modis-china-visit/articleshow/47211268.cms; and Richard M. Rossow, "India's Trade Reality: Good Trade Imbalance with China Spikes," *U.S.–India Insight* 5, no. 6 (June 2015), http://csis.org/files/publication/150609_USIndiaInsight_June_Clean_0.pdf.

15. Shishir Asthana, "Modi Must Address Trade Deficit Issue with China," *Business Standard* (India), 16 September 2014, http://www.business-standard.com/article/economy-policy/modi-must-address-trade-deficit-issue-with-china-114091600642_1.html.

16. Press Trust of India, "Govt Mulling Relaxing Security Rules for Chinese Investment," *Business Standard* (India), 8 February 2015, http://www.business-standard.com/article/pti-stories/govt-mulling-relaxing-security-rules-for-chinese-investment-115020800599_1.html; and Rossow, "India's Trade Reality."

17. Asthana, "Modi Must Address Trade Deficit."

18. "India Unlikely to Give China Market Economy Status: Lack of Transparency Cited as One of the Reasons for Not Granting 'Market Economy' Status to China," *Indian Express*, 16 September 2014, http://indianexpress.com/article/business/economy/india-unlikely-to-give-china-market-economy-status/.

19. Press Trust of India, "Russia, India, China Stand United to Bring Perpetrators of Terror Acts to Justice," *Economic Times* (India), 2 February 2015, http://articles.economictimes.indiatimes.com/2015-02-02/news/58711799_1_shanghai-cooperation-organisation-trilateral-cooperation-early-conclusion; and Srinath Raghavan, "India's Tango with the Great Powers" *The Hindu* (India), 7 February 2015, http://www.thehindu.com/opinion/lead/lead-article-indias-tango-with-the-great-powers/article6866029.ece.

20. Alonso Soto and Anthony Boadle, "BRICS Set up Bank to Counter Western Hold on Global Finance," *Reuters*, 16 July 2014, http://in.reuters.com/article/2014/07/15/brics-summit-bank-idINKBN0FK08620140715; Shyam Saran, "The Asian Future of Reserves," *Business Standard* (India), 16 May 2012, http://www.business-standard.com/article/opinion/shyam-saran-the-asian-future-of-reserves-112051600009_1.html; and Jabin T. Jacob, *India's China Policy: Time to Overcome Political Drift* (Singapore: S. Rajaratnam School of International Studies, Nanyang Technological University, June 2012).

21. Kathryn Hochstetler and Manjana Milkoreit, "Emerging Powers in the Climate Negotiations: Shifting Identity Conceptions," *Political Research Quarterly* 67, no.1 (2014) 224–35; Press Trust of India, "BASIC Countries Ask Developed Nations to Walk the Talk for Climate Change," *Economics Times* (India), 8 August 2014, http://articles.economictimes.indiatimes.com/2014-08-08/news/52594367_1_environmental-affairs-edna-molewa-durban-platform-climate-change; and Reed Landberg, "China, India Push Rich Countries to Move First on Climate Change," *Bloomberg*, 20 November 2013, http://www.bloomberg.com/news/articles/2013-11-20/china-india-prod-rich-nations-to-move-first-on-global-warming.

22. Niranjan Rajadhyaksha, "For a Himalayan Consensus," *livemint*, 29 September 2009, http://www.livemint.com/Opinion/PoN8MamCLrBesgTXIVG9CM/For-a-Himalayan-consensus.html.

23. Vishwa Mohan, "US Rules Out China-like Climate Deal with India in Near Future," *Times of India*, 11 December 2014, http://timesofindia.indiatimes.com/home/environment/global-warming/US-rules-out-China-like-climate-deal-with-India-in-near-future/articleshow/45472132.cms.

24. Government of the Republic of India and Government of the People's Republic of China, "Joint Statement on Climate Change between India and China during Prime Minister's Visit to China" (press release, Ministry of External Affairs, Government of India, 15 May 2015), http://www.mea.gov.in/bilateral-documents.htm?dtl/25238/Joint_Statement_on_Climate_Change_between_India_and_China_during_Prime_Ministers_visit_to_China; and Antto Vihma, "India and the Global Climate Governance: Between Principles and Pragmatism," *Journal of Environment & Development* 20, no.1 (2011): 69–94.

25. Rakesh Chopra, "Book Review: Energy and Security in South Asia: Cooperation or Conflict," *Journal of Defence Studies* 8, no. 4 (October–December 2014), 57.

26. Hu Shisheng, Raffaello Pantucci, and Ravi Sawhney, "A Roadmap for Sino–Indian Cooperation in Afghanistan," *Contemporary International Relations* 24, no. 3 (May–June 2014), 17, 22.

27. Ibid., 20, 24.

28. Richard Weitz, "Assessing China's Afghan Peace Play," *China Brief* 14, no. 23, (5 December 2014), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=43158&cHash=cdf9d3723aea6491802a49aad8f898be#.VQdS7d5KOfU.

29. India claims 38,000 square km (km^2) of territory in Aksai Chin that is held by China, as well as 5,180 km^2 of territory in the Shaksgam Valley that Pakistan handed over to China in 1963. Meanwhile, China claims 90,000 km^2 of Arunachal Pradesh. China refuses recognition

of the McMahon Line along the eastern border (in Arunachal Pradesh) as per the terms of the 1914 Simla Accord and the Ardagh–Jonhson Line along the western border (in Aksai Chin).

30. Rahul Singh, "China Ends Ladakh Standoff, Troops Pull Back," *Hindustan Times* (India), 5 May 2013, http://www.hindustantimes.com/newdelhi/china-ends-ladakh-standoff-troops-pull-back/article1-1055249.aspx; and Rumel Dahiya, "Border Standoff: Understanding Chinese Motives" (comment, Institute for Defence Studies and Analyses, 29 September 2014), http://www.idsa.in/idsacomments/BorerStandoff_rdahiya_290914.html.

31. China has made several offers to resolve the border dispute through a territorial swap. Chinese Premier Zhou Enlai made such an offer during his 1960 visit to India. In 1979 Chinese leader Deng Xiaoping made a similar offer for a "package solution" during Indian Foreign Minister Atal Bihari Vajpayee's visit to Beijing. On both occasions, India's reluctance to equate the two sectors led to a lack of progress.

32. Richard Fenny, "Tibetan Freedom Struggle Reflects 'Polarity of Voices,' Says Dalai Lama," *Radio Free Asia*, 4 September 2014, http://www.rfa.org/english/news/tibet/voices-09042014171310.html.

33. Bhartendu Kumar Singh, "Chinese Views on the Kargil Conflict," *Institute of Peace and Conflict Studies*, no. 211, 25 June 1999.

34. Press Trust of India, "Chinese Soldiers Present in PoK," *Times of India*, 19 September 2012, http://timesofindia.indiatimes.com/india/Chinese-soldiers-present-in-PoK-Army-Chief/articleshow/16464272.cms; and Arun Joshi, "Pak's Gilgit Lease to China Catches Indian Army Unawares," *Hindustan Times* (India), 23 February 2012, http://www.hindustantimes.com/chandigarh/pak-s-gilgit-lease-to-china-catches-indian-army-unawares/article1-815671.aspx.

35. Saeed Shah and Jeremy Page, "China Readies $46 Billion for Pakistan Trade Route," *Wall Street Journal*, 16 April 2015, http://www.wsj.com/articles/china-to-unveil-billions-of-dollars-in-pakistan-investment-1429214705.

36. "Xi Refuses 'Stapled Visa' Roll Back, Modi Says No to 'One China'" *Deccan Herald* (India), 19 September 2014, http://www.deccanherald.com/content/431781/xi-refuses-039stapled-visa039-roll.html.

37. World Bank, "GDP, PPP (current international $)," 2015, accessed 14 September 2014, http://data.worldbank.org/indicator/NY.GDP.MKTP.PP.CD/countries/order%3Dwbapi_data_value_2013%20wbapi_data_value%20wbapi_data_value-last?order=wbapi_data_value_2012%20wbapi_data_value%20wbapi_data_value-last&sort=desc&display=default; and Stockholm International Peace Research Institute (SIPRI), "SO {RO Military Expenditure Database," 2015, http://www.sipri.org/research/armaments/milex/milex_database.

38. Gurmeet Kanwal, "Going Slow on Defence" *The Tribune* (India), 23 February 2015, http://www.tribuneindia.com/news/comment/going-slow-on-defence/45498.html; Kapil Patil, "India's New Mountain Strike Corps: Conventional Deterrence," *The Diplomat* (Japan), 8 August 2013, http://thediplomat.com/2013/08/indias-new-mountain-strike-corps-conventional-deterrence; Nitin A. Gokhale, "India–China Border Engagement," *Diplomat* (Japan), 14 August 2014, http://thediplomat.com/2014/08/india-china-border-engagement/; and Reuters, "With Eye on China, India to Develop Border Region," *Times of India*, 15 September 2014, http://timesofindia.indiatimes.com/india/With-eye-on-China-India-to-develop-border-region/articleshow/42509964.cms.

39. Brahma Chellaney, *Water: Asia's New Battleground*, (Washington, DC: Georgetown University Press, 2011).

40. Kanti Bajpai, "China–India Relations If Narendra Modi Wins the Indian Elections," *China-India Brief* (Singapore), no. 27, 27 April–13 May 2014, http://lkyspp.nus.edu.sg/cag

/publication/china-india-brief/china-india-brief-27; and Rup Narayan Das, "Modi Faces Pressing Questions about India's China Policy," *China Brief: A Journal of Analysis and Information* 14, no. 10 (23 May 2014), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=42412&cHash=46ac1342575010790782d2f97679f903.

41. Press Trust of India, "China President Xi's India Visit;" and Debaisish Roy Chowdhury, "Why Modi's India is Warming to China," *South China Morning Post* (Hong Kong), 17 September 2014, http://www.scmp.com/news/china/article/1594227/why-modis-india-warming-china.

42. Indrani Bagchi, "Tibetan Leader at Modi's Swearing in Irks China," *Times of India*, 5 June 2014, http://timesofindia.indiatimes.com/india/Tibetan-leader-at-Modis-swearing-in-irks-China/articleshow/36080500.cms.

43. Nayanima Basu, "China Dashes $100-bn Hope, to Invest $20 BN over 5 Years," *Business Standard* (India), 19 September 2014, http://www.business-standard.com/article/economy-policy/china-dashes-100-bn-hope-to-invest-20-bn-over-5-years-114091800557_1.html.

44. "China Premier Li Keqiang in India for First Foreign Trip," *BBC*, 19 May 2013, http://www.bbc.co.uk/news/world-asia-22585466; Press Trust of India, "Chinese Foreign Minister Wang Yi Holds Talks with Sushma Swaraj," *Times of India*, 8 June 2014, http://timesofindia.indiatimes.com/india/Chinese-foreign-minister-Wang-Yi-holds-talks-with-Sushma-Swaraj/articleshow/36241519.cms; and "China's Xi Jinping Signs Landmark Deals on India Visit," *BBC*, 18 September 2014, http://www.bbc.co.uk/news/world-asia-india-29249268.

45. Eric Meyer, "Who Sabotaged Chinese President Xi Jinping's India Visit?," *Forbes*, 23 September 2014, http://www.forbes.com/sites/ericrmeyer/2014/09/23/who-sabotaged-xi-jinpings-india-visit/; and Manoj Joshi, "Making Sense of the Depsang Incursion" *The Hindu* (India), 7 May 2013, http://www.thehindu.com/opinion/op-ed/making-sense-of-the-depsang-incursion/article4689838.ece.

46. Cheng Li, "The Last Year of Hu's Leadership: Hu's to Blame," *China Brief* 11, no. 23 (20 December 2011), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=38811&cHash=c0006cd99bfe551991fcf1924d37c0cf#.VQRMTN5KPUp.

47. Shen Dingli, "With Xi's New Power Is Collective Leadership Over?," *East Asia Forum*, 19 October 2014, http://www.eastasiaforum.org/2014/10/19/with-xis-new-power-is-collective-leadership-over/.

48. "Military Corruption: Rank and Vile," *Economist*, 14 February 2015, http://www.economist.com/news/china/21643225-xi-jinping-flexes-his-muscle-against-army-corruption-rank-and-vile.

49. See Reshma Patil, *Strangers across the Border: Indian Encounters in Boomtown China* (Noida: Harper Collins India, 2014); and Pallavi Aiyar, *Smoke and Mirrors: An Experience of China* (New Delhi: Fourth Estate, 2008).

50. For example "India–China Relations and The Media: Blame the Messenger," *Banyan* (blog), on the *Economist* web site, 21 May 2012, http://www.economist.com/blogs/banyan/2012/05/india-china-relations-and-media; Debasish Roy Chowdhury, "Indian Press Buries Truth at the Border," *Asia Times*, 18 February 2012, http://www.atimes.com/atimes/South_Asia/NB18Df01.html; D. S. Rajan, "China Should Break up the Indian Union, Suggests a Chinese Strategist," C3S Paper, no. 325 (Chennai, India: Chennai Centre for Strategic Studies, 9 August 2009), http://www.c3sindia.org/india/719; and Press Trust of India, "Nervous China May Attack India by 2012: Expert," *Times of India*, 12 July 2009, http://timesofindia.indiatimes.com/india/Nervous-China-may-attack-India-by-2012-Expert/articleshow/4769593.cms.

51. Ministry of External Affairs, Government of India, "Joint Statement between the India and China during Prime Minister's visit to China" (press release, 15 May 2015), http://www.mea.gov.in/bilateral-documents.htm?dtl/25240/Joint_Statement_between_the_India_and_China_during_Prime_Ministers_visit_to_China.

52. Ravi Mishra, "India to Outstrip China in Long-Term Growth," *China-India Brief* (Singapore), no. 43, 13–27 January 2015, http://lkyspp.nus.edu.sg/cag/publication/china-india-brief/china-india-brief-43.

53. Ibid.

54. Ministry of External Affairs, "Joint Statement between the India and China."

55. Geoffrey Till, *Asia's Naval Expansion: An Arms Race in the Making?* (London: International Institute for Strategic Studies, 2012), 47.

56. Victor Mallet, "India Plays Soft Power Game in China's Backyard," *Financial Times*, 18 May 2015, http://www.ft.com/cms/s/0/c72967f8-fd52-11e4-b072-00144feabdc0.html.

57. Prime Minister Narendra Modi at the Tsinghua University, Beijing (address, 15 May 2015), http://www.mea.gov.in/Speeches-Statements.htm?dtl/25242/Address_by_Prime_Minister_at_the_Tsinghua_University_Beijing_May_15_2015.

58. Pieter D. Wezeman and Siemon T. Wezeman, "SIPRI Fact Sheet: Trends in International Arms Transfers, 2014" (fact sheet, Stockholm International Peace Research Institute, March 2015), http://books.sipri.org/files/FS/SIPRIFS1503.pdf.

59. Farhan Bokhari and Charles Clover, "Pakistan Nears Deal to Buy 8 Chinese Submarines," *Financial Times*, 1 April 2015, http://www.ft.com/cms/s/0/a2c22012-d845-11e4-ba53-00144feab7de.html.

60. Manu Pubby, "India Kicks Off Trilateral Talks with Japan and Australia: Joint Training, Naval Exercises on Agenda," *Economic Times* (India), 8 June 2015, http://economictimes.indiatimes.com/news/defence/india-kicks-off-trilateral-talks-with-japan-and-australia-joint-training-naval-exercises-on-agenda/articleshow/47579881.cms; and David Scott, "India's New Trilateral with Australia and Japan: China-Centric Nuances," *China-India Brief* 54, 24 June–15 July 2015, http://lkyspp.nus.edu.sg/cag/publication/china-india-brief/china-india-brief-54.

61. Pranab Dhal Samanta, "India-China Face-off Worsens over ADB Loan for Arunachal, Bank Doesn't Help," *Indian Express*, 15 May 2009, http://archive.indianexpress.com/news/indiachina-faceoff-worsens-over-adb-loan-for-arunachal/459910/.

62. George J. Gilboy and Eric Heginbotham, *Chinese and Indian Strategic Behavior: Growing Power and Alarm* (New York: Cambridge University Press, 2012).

63. For definition of *security dilemma*, see Robert Jervis, "Cooperation under the Security Dilemma," *World Politics* 30, no. 2 (January 1978): 167–214.

64. Rahul Roy-Chaudhury, "Sea's the Limit," *Force*, 6 August 2013, http://www.forceindia.net/SeastheLimit.aspx.

65. Shashank Joshi, "China and India: Awkward Ascents," *Orbis* 55, no. 4 (Fall 2011), 566.

66. US Energy Information Administration, *Country Analysis Briefs: China,* November 2010–2011, https://web.archive.org/web/20140116153042/http://www.eia.gov/countries/country-data.cfm?fips=CH&trk=m; Oystein Tunsjo, *Security and Profit in China's Energy Policy: Hedging Against Risk* (New York: Columbia University Press, 2013), 147; and Office of Naval Intelligence (ONI), *The PLA Navy: New Capabilities and Missions for the 21st Century* (Suitland, MD: ONI, 2015), 11.

67. Ian Storey, "China's "Malacca Dilemma," *China Brief* 6, no. 8 (2006), http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=3943&no_cache=1#.VB61yRZnzjA.

68. State Council Information Office, People's Republic of China, *China's Military Strategy 2014*, white paper (Beijing: PRC, May 2015), http://eng.mod.gov.cn/Database/WhitePapers/; Aki Nakai, *Occasional Papers on Asia: China's Naval Modernisation: Reflections on a Symposium* (Boston: Boston University Center for the Study of Asia, February 2011), 8; and Nan Li, "The Evolution of China's Naval Strategy and Capabilities: From 'Near Coast' and 'Near Seas' to 'Far Seas,'" *Asian Security* 5 no. 2 (2009): 144–69.

69. Office of Naval Intelligence, *The PLA Navy*, 7.

70. Rajat Pandit, "Presidential Fleet Review: India Showcases Maritime Might," *Times of India*, 21 December 2011, http://timesofindia.indiatimes.com/india/ampnbspPresidential-Fleet-Review-India-showcases-maritime-might/articleshow/11187148.cms?; Integrated Headquarters (Navy), *Freedom to Use the Seas: India's Maritime Military Strategy* (New Delhi: Ministry of Defence, 2007), 59, http://www.irfc-nausena.nic.in/irfc/ezine/maritime_strat.pdf; and Walter C. Ladwig III, "Delhi's Pacific Ambition: Naval Power, 'Look East,' and India's Emerging Influence in the Asia–Pacific," *Asian Security* 5, no. 2 (2009): 87–113, http://users.ox.ac.uk/~mert1769/Pacific%20Ambition.pdf.

71. Iskander Rehman, "An Ocean at the Intersection of Two Emerging Maritime Narratives," *IDSA Issue Brief*, 11 July 2011, http://idsa.in/issuebrief/AnOceanatTheIntersectionofTwoEmergingMaritimeNarratives; and Ladwig, "Delhi's Pacific Ambition: Naval Power."

72. K. M. Panikkar, *India and Indian Ocean: An Essay on the Influence of Sea Power on Indian History* (London: George Allen & Unwin Ltd, 1951); and James Holmes and Toshi Yoshihara, "Liu Huaqing, RIP," *The Diplomat* (Japan), 18 January 2011, http://thediplomat.com/2011/01/liu-huaqing-rip/.

73. Willy Lam, "Beijing Adopts Multi-Pronged Approach to Parry Washington's Challenge," *China Brief* 11, no. 22, 30 November 2011, http://www.jamestown.org/single/?tx_ttnews%5Btt_news%5D=38715&no_cache=1#.VfGML3DBzGc.

74. The first island-chain refers to a line through the Kurile Islands, Japan, the Ryukyu Islands, Taiwan, the Philippines, and Indonesia. The second island-chain extends to Guam and Indonesia, including the Bonins, Marianas, and the Carolines and encompassing an area of 1,800 nautical miles from China's coast.

75. Office of Naval Intelligence, *The PLA Navy*, 30; Huang Jingjing, "China Announces Pacific Drill," *Global Times* (China), 25 November 2011, http://www.globaltimes.cn/content/685720.shtml; and Emanuele Scimia, "China's Influence Spreads to Atlantic," *Asia Times* (Hong Kong), 20 May 2013, http://www.atimes.com/atimes/China_Business/CBIZ-01-200513.html.

76. Elizabeth Wishnick, "Russia and China Go Sailing," *Foreign Affairs*, 26 May 2015, https://www.foreignaffairs.com/articles/china/2015-05-26/russia-and-china-go-sailing.

77. Indian Adm Nirmal Verma, quoted in Indian Navy, "New Naval Air Station 'INS Baaz' Commissioned by CNS" (press release, Indian Navy, 31 July 2012), http://indiannavy.nic.in/print/1431.

78. Ajai Shukla, "New Naval Base Coming up Near Visakhapatnam," *Business Standard* (India), 26 August 2014, http://www.business-standard.com/article/current-affairs/new-naval-base-coming-up-near-visakhapatnam-114082601458_1.html.

79. Office of Naval Intelligence, *The PLA Navy*, 13.

80. Srinivas Mazumdaru, "Naval Buildup Reflects India's 'Ambition to Project Power," *Deutsche Welle*, 23 February 2015, http://www.dw.com/en/naval-buildup-reflects-indias-ambition-to-project-power/a-18275292.

81. Tom Phillips, "China Silently Forges Ahead with Second Aircraft Carrier," *Telegraph* (United Kingdom), 3 February 2015, http://www.telegraph.co.uk/news/worldnews/asia/china/11385864/China-silently-forges-ahead-with-second-aircraft-carrier.html.

82. Richard Bitzinger, "Aircraft Carriers: China's Emerging Maritime Ambitions," *RSIS Commentaries*, 7 April 2009, https://www.rsis.edu.sg/wp-content/uploads/2014/07/CO09035.pdf.

83. "Indian Navy Chief Admiral Sureesh Mehta Spells Out Vision 2022," *India Defence*, 10 August 2008, https://web.archive.org/web/20100504203650/http://www.india-defence.com/reports/3954; and Mazumdaru, "Naval Buildup Reflects India's 'Ambition.' "

84. Office of Naval Intelligence, *The PLA Navy*, 23.

85. Kris Osborn, "China Unveils Three New Nuclear-Powered Attack Submarines," *Defense Tech*, 3 April 2015, http://defensetech.org/2015/04/03/china-unveils-three-new-nuclear-powered-attack-submarines/#more-24736.

86. Megan Eckstein, "India Launches First Indigenously Built Attack Submarine" *USNI News*, 6 April 2015, http://news.usni.org/2015/04/06/india-launches-first-indigenously-built-attack-submarine.

87. Office of Naval Intelligence, *The PLA Navy*, 5; and Mazumdaru, "Naval Buildup Reflects India's 'Ambition.' "

88. Toshi Yoshihara, "The US Navy's Indo-Pacific Challenge," *Journal of the Indian Ocean* 9, no. 1 (2013), 92.

89. C. Raja Mohan, *Samudra Manthan: Sino–Indian Rivalry in the Indo-Pacific* (Washington, DC: Carnegie Endowment for International Peace, 2012), 9.

90. Ibid., xii.

91. Ibid., 205.

92. Indian Navy, *Indian Maritime Doctrine 2009* (New Delhi: Ministry of Defence, 2009), 75.

93. Manash Pratim Bhuyan, "India Favours Freedom of Navigation in South China Sea," *Outlook* (India), 10 August 2014, http://www.outlookindia.com/news/article/India-Favours-Freedom-of-Navigation-in-South-China-Sea/854509; Ralf Emmers, "The US Rebalancing Strategy: Impact on the South China Sea" (occasional brief, Australian National University, 30 October 2013), http://nsc.anu.edu.au/documents/occasional-5-brief-8.pdf; and Tetsuo Kotani, "The Senkaku Islands and the US-Japan Alliance: Future Implications for the Asia-Pacific," *Project 2049 Institute*, 19 September 2013, http://project2049.net/documents/senkaku_kotani.pdf.

94. Office of the Press Secretary, White House, "U.S.-India Joint Strategic Vision for the Asia-Pacific and Indian Ocean Region" (press release, White House, 25 January 2015), http://www.whitehouse.gov/the-press-office/2015/01/25/us-india-joint-strategic-vision-asia-pacific-and-indian-ocean-region.

95. Vivek Raghuvanshi, "India-Japan Talks to Focus on Strategic Talks, Possible Aircraft Deal," *DefenseNews,* 28 August 2014, http://www.defensenews.com/article/20140828/DEFREG03/308280038/India-Japan-Talks-Focus-Strategic-Ties-Possible-Aircraft-Deal; and Press Trust of India, "India, Japan to Hold First Bilateral Naval Exercise off Tokyo," *Deccan Herald* (India), 4 June 2012, http://www.deccanherald.com/content/254462/india-japan-hold-first-bilateral.html.

96. Indrani Bagchi, "India Ignores China's Frown, Offers Defence Boost to Vietnam," *Times of India*, 29 October 2014, http://timesofindia.indiatimes.com/india/India-ignores-Chinas-frown-offers-defence-boost-to-Vietnam/articleshow/44965272.cms; Ankit Panda, "India-Vietnam Supersonic Missile Talks in 'Advanced Stage,' *The Diplomat* (Japan), 15 September

2014, http://thediplomat.com/2014/09/india-vietnam-hypersonic-missile-talks-in-advanced-stage/; and The Hanoist, "Vietnam Builds Naval Muscle," *Asia Times* (Hong Kong), 29 March 2012, http://www.atimes.com/atimes/Southeast_Asia/NC29Ae01.html.

97. Ben Bland and Girija Shivakumar, "China Confronts Indian Navy Vessel," *Financial Times*, 31 August 2011, http://www.ft.com/intl/cms/s/0/883003ec-d3f6-11e0-b7eb-00144feab49a.html#axzz3lLANH4dM.

98. Ananth Krishna, "In South China Sea a Surprise Chinese Escort for Indian Ships," *The Hindu* (India), 14 June 2012, http://www.thehindu.com/news/national/in-south-china-sea-a-surprise-chinese-escort-for-indian-ships/article3524965.ece; and "The Indian Navy in the South China Sea: Beijing's Unwelcome Escort," *Indian Express*, 14 June 2012.

99. Vu Trong Khanh and Nguyen Anh Thu, "Vietnam, India to Expand Oil Exploration in Contested South China Sea," *Wall Street Journal*, 15 September 2014, http://online.wsj.com/articles/vietnam-india-to-expand-oil-exploration-in-contested-south-china-sea-1410777168; and The Hanoist, "Great Game in the South China Sea," *Asia Times* (Hong Kong), 17 April 2012, http://www.atimes.com/atimes/Southeast_Asia/ND17Ae01.html.

100. Shannon Tiezi, "China Pushes 'Maritime Silk Road' in South, Southeast Asia," *The Diplomat* (Japan), 17 September 2014, http://thediplomat.com/2014/09/china-pushes-maritime-silk-road-in-south-southeast-asia/.

101. Ibid; and Wu Jiao and Zhang Yunbi, "Xi in Call for Building of New 'Maritime Silk Road'," *China Daily*, 4 October 2013, http://usa.chinadaily.com.cn/china/2013-10/04/content_17008940.htm.

102. Nuwan Peiris, "China, India in Race to Exploit Indian Ocean Seabed," *Sunday Times* (Sri Lanka), 15 December 2013, http://www.sundaytimes.lk/131215/sunday-times-2/china-india-in-race-to-exploit-indian-ocean-seabed-76395.html.

103. Chow Chung-yan, "Chinese Navy Sees Off Indian Sub," *South China Morning Post* (Hong Kong), 4 February 2009, http://www.scmp.com/article/668780/chinese-navy-sees-indian-sub.

104. Sandeep Unnithan, "Exclusive: Indian Navy Headless as Chinese Nuclear Sub Prowls Indian Ocean," *India Today*, 21 March 2014, http://indiatoday.intoday.in/story/indian-navy-chinese-nuclear-sub-indian-ocean/1/350498.html; Abhijit Singh, "A 'PLA-N' for Chinese Maritime Bases in the Indian Ocean," *PacNet* 7, 26 January 2015, http://csis.org/files/publication/Pac1507.pdf; and Toshi Yoshihara, "Undersea Dragons in the Indian Ocean?," *China-India Brief* 37, 14–28 October 2014, http://lkyspp.nus.edu.sg/cag/publication/china-india-brief/china-india-brief-37.

105. John Garver, "The Security Dilemma in Sino–Indian Relations," *India Review* 1, no. 4 (October 2002): 33–34.

106. N. C. Bipindra, "India to Unveil First Warship to Deter Chinese Submarines," *Bloomberg BusinessWeek*, 22 August 2014, http://www.businessweek.com/news/2014-08-21/india-to-unveil-warship-to-deter-chinese-submarines-near-coast.

107. Shannon Tiezzi, "The Maritime Silk Road vs. The String of Pearls," *The Diplomat* (Japan), 13 February 2014, http://thediplomat.com/2014/02/the-maritime-silk-road-vs-the-string-of-pearls/; Jiao and Yunbi, "Xi in Call for Building;" and James Crabtree, "Sri Lanka Sees Benefits of China's 'Maritime Silk Road' Plan," *Financial Times*, 17 September 2014, http://www.ft.com/intl/cms/s/0/8645737e-3e2d-11e4-b7fc-00144feabdc0.html.

108. Abhijit Singh, "China's 'Maritime Bases' in the IOR: A Chronicle of Dominance Foretold," *Strategic Analysis* 39, no. 3 (2015): 293–97; "Chinese Paper Advises PLA Navy to Build Overseas Military Bases," *China Defence Mash-up*, 13 January 2013, http://www.china-defense-mashup.com/chinese-paper-advises-pla-navy-to-build-overseas-military-bases.html;

and Andrew S. Erickson and Gabriel Collins, "Dragon Tracks: Emerging Chinese Access Points in the Indian Ocean," *AMTI Brief*, 18 June 2015, http://amti.csis.org/dragon-tracks-emerging-chinese-access-points-in-the-indian-ocean-region/; and Mohan, *Samudra Manthan*, 67.

109. Mohan, *Samudra Manthan*, 135.

110. Indrani Bagchi, "India Looks East, to Vietnam and Myanmar," *Times of India*, 8 October 2011, http://timesofindia.indiatimes.com/india/India-looks-east-to-Vietnam-and-Myanmar/articleshow/10273422.cms.

111. Michael S. Chase and Andrew S. Erickson, "Changes in Beijing's Approach to Overseas Basing?," *China Brief* 9, no. 19 (24 September 2009), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=35536&cHash=77d682d109#.VfGcgXDBzGc.

112. Mohan, *Samudra Manthan*, chapter 8.

113. C. Raja Mohan, "Modi and the Indian Ocean: Restoring India's Sphere of Influence," *AMTI Brief*, 18 June 2015, http://amti.csis.org/modi-and-the-indian-ocean-restoring-indias-sphere-of-influence/; and Tom Mitchell, "Sri Lanka to Review Terms of Chinese Loans," *Financial Times*, 28 February 2015, http://www.ft.com/intl/cms/s/0/c582f4a6-bf49-11e4-99f8-00144feab7de.html.

114. Press Trust of India, "China President Xi's Visit: India to Hold Maritime Dialogue with China this Year," *Economic Times* (India), 18 September 2014, http://articles.economictimes.indiatimes.com/2014-09-18/news/54067931_1_south-china-sea-maritime-dialogue-navigation; and Ashok Tuteja, "India, China to Kickstart Maritime Dialogue," *Tribune* (India), 14 April 2012, http://www.tribuneindia.com/2012/20120414/nation.htm#1.

115. Shivshankar Menon, "India's NSA on Sino–Indian Rivalry in the Indo–Pacific," *Observer Research Foundation*, 4 March 2013, 2, http://www.orfonline.org/cms/export/orfonline/documents/Samudra-Manthan.pdf.

116. Roughly 38 Indian Navy vessels were deployed to provide humanitarian assistance in the aftermath of the Indian Ocean tsunami, with five operations in Indonesia, Sri Lanka, Maldives, and off the Indian coast.

117. From April to September 2002, the Indian Navy escorted more than 20 vessels through the Strait of Malacca as part of Operation Enduring Freedom.

118. Rahul Roy-Chaudhury, "India: Gulf Security Partner in Waiting?," in *Middle Eastern Security, US Pivot and the Rise of ISIS*, edited by Toby Dodge and Emile Hokayem (Oxon: Routledge, 2014), 235.

119. Prashanth Parameswaran, "Modi Unveils India's 'Act East Policy' to ASEAN in Myanmar," *The Diplomat* (Japan), 17 November 2014, http://thediplomat.com/2014/11/modi-unveils-indias-act-east-policy-to-asean-in-myanmar; and C. Raja Mohan, "Not So Easy to Act East," *Indian Express*, 22 November 2014, http://indianexpress.com/article/opinion/columns/not-so-easy-to-act-east/.

120. Scott Cheney-Peters, "India's Maritime Acts in the East" *AMTI Brief*, 18 June 2015, http://amti.csis.org/indias-maritime-acts-in-the-east/.

121. Jesse Karotkin, "PLAN Shapes International Perception of Evolving Capabilities," *China Brief* 10, no. 3 (4 February 2010), http://www.jamestown.org/programs/chinabrief/single/?tx_ttnews%5Btt_news%5D=36008&cHash=7169dd6cdc#.VfGe_nDBzGc; and Information Office of the State Council, People's Republic of China, *China's National Defense in 2008*, white paper (Beijing: PRC, 2009), http://carnegieendowment.org/files/2008DefenseWhitePaper_Jan2009.pdf.

122. Office of Naval Intelligence, *PLA Navy*, 29; and Peter Layton, "China's Velvet Fist: PLA in Operations-Other-Than-War," *Defence Today*, November 2012, https://www.academia.edu/2307749/China_s_velvet_fist_PLA_in_operations-other-than-war.

123. "Chinese Hospital Ship Back after Treating Thousands," *China Daily*, 27 November 2010, http://www.china.org.cn/china/2010-11/27/content_21434218.htm; and Office of Naval Intelligence, *The PLA Navy*, 10.

124. Office of Naval Intelligence, *The PLA Navy*, 30.

125. Shivshankar Menon, "The Evolving Balance of Power in Asia" (paper, presented to IISS Global Strategic Review, Geneva, 13 September 2009).

126. Luis Simón, "Reaching Beyond the Indo-Pacific," *Comparative Strategy* 32, no. 4 (2013), 337, https://www.academia.edu/7851546/Reaching_Beyond_the_Indo-Pacific.

127. Scott Kennedy and David A. Parker "Building China's 'One Belt, One Road,'" *CSIS* (web site), 3 April 2015, http://csis.org/publication/building-chinas-one-belt-one-road.

128. Ibid., and Simon, "Reaching Beyond."

129. Zorawar Daulet Singh, "China Strategy: Mackinder versus Mahan," *Tribune* (India), 26 April 2013, http://www.tribuneindia.com/2013/20130426/edit.htm#7.

130. Zorawar Daulet Singh, "Indian Perceptions of China's Maritime Silk Road Idea," *Journal of Defence Studies* 8, no. 4 (October–December 2014), 140.

131. Till, *Asia's Naval Expansion*, 202.

132. Stephen Smith, "Speech by Stephen Smith MP Minister for Defence, 'Australia and India Building the Strategic Partnership,' at the Asia Society, Mumbai," Department of Defence (Australia), 2011. http://www.minister.defence.gov.au/2011/12/10/minister-for-defence-australia-and-india-building-the-strategic-partnership.

133. Rory Medcalf, "In Defence of the Indo-Pacific: Australia's New Strategic Map," *Australian Journal of International Affairs* 68, no. 4 (2014), 472.

134. Bloomberg, "China Seeking to be 'New Force' in Mideast Peace," *South China Morning Post*, 20 June 2013, http://www.scmp.com/news/china/article/1264596/china-seeking-be-new-force-mideast-peace; and "India to Step Up Oil Import from Africa: Minister," *Xinhua*, 10 December 2011, http://news.xinhuanet.com/english/business/2011-12/10/c_131298486.htm.

135. John Mitchell, *Asia's Oil Supply: Risks and Pragmatic Remedies* (London: Chatham House, May 2014), 2, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20140506Asia%27sOilSupplyMitchell.pdf.

136. Nima Khorrami Assl, "China and India: Rival Middle East Strategies," *Al Jazeera,* 10 January 2012, http://www.aljazeera.com/indepth/opinion/2012/01/20121811164584439.html.

137. For the origins of the US "strategic pivot/re-balancing" toward Asia, see Hillary Clinton, secretary of state, "America's Engagement in the Asia-Pacific" (address, Honolulu, HI, 28 October 2010), http://m.state.gov/md150141.htm; Hillary Clinton, "America's Pacific Century," *Foreign Policy*, 11 October 2011, http://foreignpolicy.com/2011/10/11/americas-pacific-century/; Barack Obama, "Remarks by President Obama to the Australian Parliament" (address, Parliament House, Canberra, Australia, 17 November 2011), https://www.whitehouse.gov/the-press-office/2011/11/17/remarks-president-obama-australian-parliament; and Tom Donilon, "The United States and the Asia-Pacific in 2013" (address, Asia Society, 11 March 2013), http://www.whitehouse.gov/the-press-office/2013/03/11/remarks-tom-donilon-national-security-advisory-president-united-states-a.

138. John Mitchell, *Asia's Oil Supply*.

139. Ibid.

140. Ibid, 11.

141. Mohan Guruswamy, "India-China War Delayed by Technology," *Asia Times* (Hong Kong), 7 May 2013, http://www.atimes.com/atimes/South_Asia/SOU-02-070513.html.

142. See Christopher M. Davidson, "The Gulf Monarchies and Pacific Asia: Towards Interdependency?," in *Converging Region: Global Perspectives on Asia and the Middle East*, edited by Nele Lenze and Charlotte Schriwer (Surrey, UK: Ashgate, 2014), 143–60.

143. Guruswamy, "India-China War Delayed by Technology."

144. Prasanta Kumar Pradhan, "Accelerating India's 'Look West Policy' in the Gulf," *Institute of Defence Studies and Analyses Issue Brief*, 3 February 2011, http://www.idsa.in/issuebrief/AcceleratingIndiasLookWestPolicyintheGulf.html.

145. John Calabrese, "From Flyswatters to Silkworms: The Evolution of China's Role in West Asia," *Asian Survey* 30, no. 9 (September 1990), 872–75.

146. Alexander Neill, "China and the Middle East," in *Middle Eastern Security, the US Pivot and the Rise of ISIS*, edited by Toby Dodge and Emile Hokayem (Oxon: Routledge, 2014), 213–14.

147. Mohan, *Samudra Manthan*, 223; Wishnick, "Russia and China Go Sailing;" and Thoma Erdbrink and Chris Buckley, "China and Iran to Conduct Joint Naval Exercises in the Persian Gulf," *New York Times*, 21 September 2014, http://www.nytimes.com/2014/09/22/world/middleeast/china-and-iran-to-conduct-joint-naval-exercises-in-the-persian-gulf.html.

148. Michele Kambas, "Chinese Warship in Cyprus to Aid Syrian Chemical Weapons Removal," *Reuters*, 4 January 2014, http://www.reuters.com/article/2014/01/04/us-syria-crisis-china-idUSBREA0304820140104.

149. Rahul Roy-Chaudhury, "India: Gulf Security Partner in Waiting?," 229.

150. Greg Torode and Minnie Chan, "PLA Navy Ends Warship to Safeguard Libya Evacuees," *South China Morning Post* (Hong Kong), 26 February 2011, http://www.scmp.com/article/739196/pla-navy-sends-warship-safeguard-libya-evacuees.

151. Reuters, "India Ends Yemen Operations, Rescues People from 41 Nations," *Economic Times* (India), 10 April 2015, http://economictimes.indiatimes.com/news/politics-and-nation/india-ends-yemen-operations-rescues-people-from-41-nations/articleshow/46875805.cms.

152. Michelle FlorCruz, "Chinese Navy's Yemen Evacuation Draws International Praise, Highlights Navy's Global Reach," *International Business Times*, 8 April 2015, http://www.ibtimes.com/chinese-navys-yemen-evacuation-draws-international-praise-highlights-navys-global-1874313.

153. Gary Sands, "China and the ISIS Threat," *The Diplomat* (Japan), 26 September 2014, http://thediplomat.com/2014/09/china-and-the-isis-threat/; and Roy-Chaudhury, "India: Gulf Security Partner in Waiting?," 239.

154. Indo-Asian News Service, "Clinton Urges India to Play Larger Role in Asia," *Khaleej Times* (United Arab Emirates), 14 November 2012, http://www.khaleejtimes.com/article/20121114/ARTICLE/311149928/1028.

155. Bertil Lintner, "India-Myanmar: A Half-built Gateway," *Asia Times* (Hong Kong), 30 November 2011, http://www.atimes.com/atimes/Southeast_Asia/MK30Ae01.html.

156. Office of the Press Secretary, White House, "Remarks by the President to the Joint Session of the Indian Parliament" (press release, White House, 9 November 2010), http://www.whitehouse.gov/the-press-office/2010/11/08/remarks-president-joint-session-indian-parliament-new-delhi-india; Press Information Bureau, Government of India, "Joint Statement of Prime Minister Dr. Manmohan Singh and President Barack Obama," 8 November 2010, http://pib.nic.in/newsite/PrintRelease.aspx?relid=66860; and Office of the Press Secretary, White House, "U.S.-India Joint Strategic Vision for the Asia-Pacific and Indian Ocean

Region" (press release, White House, 25 January 2015), http://www.whitehouse.gov/the-press-office/2015/01/25/us-india-joint-strategic-vision-asia-pacific-and-indian-ocean-region.

157. Leon Panetta, "The U.S. and India: Partners in the 21st Century," 6 June 2012, http://spacenews.com/us-and-india-partners-21st-century/.

158. William J. Burns, "U.S.-India Partnership in an Asia-Pacific Century," 16 December 2011, http://www.state.gov/s/d/2011/178934.htm.

159. David Scott, "The 'Indo-Pacific' – New Regional Formulations and New Maritime Frameworks for US-India Strategic Convergence," *Asia-Pacific Review* 19, no. 2 (2012), 86, 100.

160. Ibid., 87.

161. Ashley Tellis, "Obama in India Building a Global Partnership: Challenges, Risks, Opportunities," *Policy Outlook*, 28 October 2010, 25, http://carnegieendowment.org/files/obama_in_india.pdf.

162. Mohan, *Samudra Manthan*, 208.

163. Tuteja, "India, China to Kickstart Maritime Dialogue."

164. For a detailed analysis of interaction between China and India during the colonial period, see Madhavi Thampi, ed., *India and China in the Colonial World* (New Delhi: Social Science Press, 2005).

165. The Association of Southeast Asian Nations's (ASEAN) Treaty of Amity and Cooperation, also known as the "ASEAN Way," centers on six principles: 1) mutual respect for the independence, sovereignty, and territorial integrity of all nations; 2) settlements of differences and disputes by peaceful means; 3) the right of every state to lead its national existence free from external interference, subversion, and coercion; 4) noninterference in the internal affairs of one another; 5) effective cooperation among member states; and 6) the renunciation of the threat and use of force.

166. Prabhakar Menon "India and the World East of It: Past and Present; An Impressionist Account," in *Two Decades of India's Look East Policy: Partnership for Peace, Progress and Prosperity*, edited by Amar Nath Ram (New Delhi: Indian Council of World Affairs, 2012), 105.

Book Reviews

Air Commanders, edited by John Andreas Olsen. Potomac Books, 2012, 542 pp., $48.00 hardcover, $28.00 paperback.

Air Commanders essentially delivers the US Air Force's combat history through the prism of selected air commanders. Despite being different in style and approach, the book is reminiscent of Benjamin Lambeth's seminal study *The Transformation of American Air Power* (2000). It is divided into three parts, each dealing with a crucial time period: World War II, the Cold War, and the period from Operation Desert Storm to Operation Iraqi Freedom. Using short biographies, each part portrays four outstanding Airmen whose individual characters and life experiences shaped major air campaigns. While some may disagree with Olsen's selection of air commanders, his choices not only allow scrutiny of the full spectrum of major USAF air campaigns but also portray very different personalities.

The interested reader recognizes a number of themes of perennial character. The most eminent is the constant fight "for a single point of contact for air management against opposition" (p. 25). In January 1944 Gen Carl A. Spaatz, the first of the commanders portrayed, met skepticism when he established a unified command in Europe, the US Strategic Air Forces headquarters. Six decades later, Gen T. Michael Moseley was convinced centralized command by an Airman was a prerequisite for effective and efficient employment of airpower.

While there are similarities over time, there are also striking differences. Fighting a war for Germany's unconditional surrender, Spaatz's biography exhibits the Airman's virtues, including a killer instinct. Quite in contrast, six decades later, Gen Michael E. Ryan's insistence to avoid collateral damage was a fulcrum of Operation Deliberate Force. Examining Lt Gen William H. Tunner's conduct of airlift operations in the China-Burma-India theater and later in the Berlin airlift, James S. Corum underscores airlift's vital role to operational success. His chapter also exhibits Tunner's foresight when it came to vital Cold War issues. In April 1960 Tunner formally advocated a flexible response doctrine supported by strategic airlift—a policy the Eisenhower administration adamantly resisted. In contrast, Gen Curtis E. LeMay was a strident proponent of massive retaliation, leaving his air force less prepared to fight a conventional war. In this regard, the biographies implicitly retrace the Cold War's fundamental strategic debates from the Airmen's perspective. Olsen's book is also corrective to the view that the USAF relationship with politics is an uneasy one. While this might have been the case in LeMay's later career, Gen John W. Vogt, architect of the Linebacker air campaigns in 1972, and General Ryan displayed subtle senses for the intricacies of politics.

The various biographies also display stark differences in leadership styles. Lt Gen George E. Stratemeyer, Gen Douglas MacArthur's air commander in the early phase of the Korean War, readily delegated tasks to capable subordinates. In the words of the editor, this "sets him apart from several other air commanders scrutinized in this book" (p. 17). While Stratemeyer was able to develop good relations with

MacArthur, frictions between their staffs persisted—a recurring theme in military command and control.

Case Cunningham aptly describes Gen William W. Momyer's talent as a tactical Airman and his effective running of centralized air operations during the battle of Khe Sanh in early 1968. His tenure as Seventh Air Force commander, from mid-1966 to mid-1968, coincided with the infamous Rolling Thunder air campaign. In contrast, General Vogt conducted the successful Linebacker air campaigns in 1972. Vogt was a highly educated officer who had gained the trust of his political superiors but was suspicious to those in theater. The chapters on Seventh Air Force commanders during the Vietnam War are symptomatic for many accounts on the air war over Vietnam. While there is undoubtedly much to say about frustrating political micromanagement, many scholars and officers alike relate the reasons for failure or success almost exclusively to US strategy and conduct of the war. Though Robert Pape remains controversial for his polarizing thesis put forward in his book *Bombing to Win*, (pp. 209–10) he convincingly argues Hanoi's strategy was at least equally important as the US conduct of the war. The communists' guerrilla strategy during the Johnson years was hardly susceptible to bombing, quite in contrast to Hanoi's conventional strategy in 1972.

With specifically focusing on the operational level of war, Olsen's ambition is to fill the void between the strategic narrative on airpower and the tactical and technical debates on aerospace issues (p. 2). While clear-cut definitions of the operational level of war are wanting, common sense suggests that operational art essentially is about orchestrating and synchronizing classical lines of operations in the various domains of warfare: land, sea, and air. This primarily is the realm of overall theater commanders, the joint force commander (JFC) in modern military parlance. Nevertheless, examining air component commanders offers specific insights into operational-level decision making. History provides ample evidence that theater commanders—mostly coming from land-centric backgrounds—devote a considerable amount of attention to the scheme of land maneuvers and neglect more effectively orchestrating the effects delivered in and out of the other domains of warfare. Since land-centric JFCs often lack a deep understanding of airpower, one of the air commanders' most eminent tasks is to develop good relationships and to provide sound advice. The dynamics between overall theater commanders and their air commanders have become perennial themes. In World War II, Maj Gen George C. Kenney and Brig Gen Otto P. Weyland had to gain the trust of their superiors—General MacArthur in the Southwest Pacific and Gen George S. Patton in the European theater, respectively. Almost six decades later, Lt Gen Chuck Horner convinced his joint force commander, Gen H. Norman Schwarzkopf, of the appropriate use of airpower. As Richard P. Hallion writes, Horner considered his superior to be "extremely intelligent" but lacking an appreciation of air and space power given his land-centric background.

To understand the US way of air warfare, a thorough grasp of its history is a prerequisite. Yet for those interested in modern military conflicts, part three of the volume is the most rewarding. The following paragraphs examine in more detail the accounts of the post–Cold War era air commanders, using the editor's ambition to provide insight into the operational level of warfare as a primary judgment criterion.

Richard P. Hallion, author of *Storm over Iraq: Air Power and the Gulf War* (1992), is undoubtedly one of the most competent airpower scholars to portray Lt Gen Charles A. "Chuck" Horner, who ushered in a new era of precision airpower. Hallion's account exhibits Horner's pragmatic approach to orchestrating the air campaign, including a sound view of the air tasking order (ATO) concept or putting forward innovative approaches such as "push close air support." Regarding the latter, Horner devised the concept anticipating the corps commanders' penchant for trying to tie up available air assets and sorties. Related to this issue is the joint force air component commander (JFACC) concept, which Desert Storm put to the test. Hallion also provides interesting insights into Col John A. Warden's actual role during planning and the Army's view on airpower and its corollaries for the conduct of the campaign. For instance, lack of understanding of modern airpower severely hampered Army efforts at effective battle damage assessment.

From an operational-level vantage point, however, the author could have strengthened the chapter by shedding light on the air-land interface during the ground offensive. Placement of the so-called fire support coordination line (FSCL) became a bone of contention between the Army and the Air Force. In essence, the ownership of the battlespace lay at its heart. Though this might not seem an overarching issue, it was identified as a point of friction by seminal studies on the Gulf War such as Thomas A. Keaney and Eliot A. Cohen's *Gulf War Air Power Survey: Summary Report* (p. 157) and *The Generals' War* by Michael Gordon and Bernard Trainor (pp. 412–13). In the aftermath of Desert Storm, it remained a sore point for the Air Force, according to a 2007 RAND report by David E. Johnson.

The author of *Responsibility of Command: How UN and NATO Commanders Influenced Airpower over Bosnia* (2003), Mark A. Bucknam, is perfectly poised to portray Gen Michael E. Ryan, air component commander of Operation Deliberate Force. Bucknam's chapter excels by providing a plethora of operational details linked to the overall strategic setting. As such, the author provides valuable insights into one of the less-commonly known air campaigns of the post–Cold War era.

Prior to the campaign, Deliberate Force planners identified 56 target sites containing a total of just 338 aim points. Ryan identified certain elements of the Bosnian Serb army as the center of gravity. Yet preserving the United Nation's (UN) backing for the air campaign and establishing a basis for a negotiated end to the war, he avoided excessive and deliberate killing of Bosnian Serb soldiers and went after heavy weapons, logistics, command and control, and mobility targets. At the same time, Ryan's goal was to destroy as many of the Bosnian Serb army's combat capabilities as possible before North Atlantic Treaty Organization (NATO) political leaders called for a halt or the Bosnian Serbs stopped the campaign by yielding to UN demands.

Bucknam exhibits Ryan's virtues and cognitive abilities to comprehensively embrace the air campaign and to control almost every aspect of targeting to avoid collateral damage. Yet he less adequately addresses the shortcomings of Ryan's leadership style. In the John C. Orndorff's study *Deliberate Force: A Case Study in Effective Air Campaigning*, (pp. 355, 372–73) the author suggests that—given Deliberate Force's limited scope—Ryan was able to exercise a centralized Napoleonic command style.

Though this approach had its merits in the particular context of Deliberate Force, Orndorff identifies potential drawbacks, most notably a tremendous amount of work placed upon a few key individuals.

Rebecca L. Grant describes Lt Gen Michael C. Short's Air Force career, which culminated in his role as combined forces air component commander in Operation Allied Force. While the 1999 air campaign went down in history as an airpower success, Grant reminds the reader that a positive outcome was anything but clear throughout most of the campaign. In particular, she highlights the doctrinal tensions between the air component commander and NATO's supreme allied commander, Europe, Gen Wesley Clark, US Army. In essence, the debate between Clark and Short was over striking so-called strategic targets in Belgrade and elsewhere in Serbia or attacking fielded forces that immediately threatened the Muslim population in Kosovo. The author appropriately highlights Army generals' lack of understanding and sometimes mistrust of airpower throughout the 1990s. As such, her chapter delivers an unvarnished and necessary account of the obstacles an Airman possibly can face in a "cross-service" chain of command. Yet the author takes it for granted that Short's preference for fixed strategic targets was correct—without providing conclusive evidence save the fact that this target set was an Airman's choice. In a similar vein, she feels empathy with Short's frustrations over the various political constraints inhibiting a more forceful air campaign from the outset.

To both issues—target set selection and gradualism, that is, not striking swift and hard—Benjamin Lambeth offers convincing answers in his authoritative study *NATO's Air War for Kosovo* (2001). Lambeth shows understanding for the air planners' view that politically driven restrictions on key targets and excessive concern for collateral damage must have been a daily source of frustration. Yet taking the view of the recipient of airpower, it seemed as if the alliance was determined to follow the bombing campaign through and to even escalate it. "The almost universal belief among air warfare professionals that a more aggressive effort starting on opening night, in consonance with a more doctrinally pristine strategy, would have yielded the same result more quickly may have been correct as far as it went, . . . but that conviction was based solely on faith in the intrinsic power of the air weapon, not on any evidence directly related to the case at hand" Lambeth argues (p. 78).

In her chapter, Grant refers to General Clark's views on the preceding NATO air campaign over Bosnia and Herzegovina. In this regard, she could have significantly strengthened her argument by also elaborating on Short's experience as General Ryan's chief of staff in Naples in 1995. In particular, as the Orndorff's study on Deliberate Force points out, then major general Short had to absorb some of the higher responsibilities that naturally might have devolved on the air component commander who, in this particular case, became deeply involved in operational-level issues at the combined air operations center at Vicenza, Italy. Though Ryan and Short both shared the frustrations of Vietnam, Ryan's view on employing airpower in 1995 and Short's view in 1999 differed significantly. Of course, the circumstances in 1995 and 1999 were also different, and there was not a set answer for dealing with the internecine wars in the Balkans.

Among the four post–Cold War air commanders portrayed, General Moseley is the only one who did not share the "traumatizing" Vietnam experience. Given Moseley's controversial "retirement" as chief of staff of the Air Force, James D. Kiras focuses his chapter on the Airman's tenure as commander of US Central Command Air Forces (USCENTAF). The chapter provides interesting insights into US approaches to joint war fighting immediately after 9/11. It particularly sheds light on Moseley's achievements in three distinct phases—Operation Anaconda (March 2002), a controversial ground-centric operation that fell short of its objective to encircle remnants of Taliban and al-Qaeda forces in the mountainous border region of Afghanistan and Pakistan; Operation Iraqi Freedom; and Operation Enduring Freedom.

While the challenge of modern joint war fighting is commonly understood as an issue primarily related to interoperable command and control systems, Kiras's chapter highlights the crucial importance of human factors in modern operations. Moseley became USCENTAF commander in November 2001—one month into Operation Enduring Freedom. According to Kiras, Moseley's predecessor was unduly blamed by the combatant commander Gen Tommy Franks, US Army, for placing Air Force priorities above those of the joint team. Moseley—by virtue of his personality—gradually gained Frank's trust, mended the air-land team, and made airpower an integral part of Operation Iraqi Freedom. Doing so, he straddled two worlds—advocating for the value of airpower while at the same time emphasizing the need to integrate it within the joint force. Kiras illustrates the latter by examining Moseley's role in making time-sensitive targeting more responsive against fleeting targets by enhancing integration between airpower and special forces. Yet the author only briefly touches on the problematic arrangements of fire support measures with conventional ground forces. As a RAND study notes: "Despite the significant improvements in ground-air effectiveness, some lingering issues remained. . . . Again, the Army deep attack concepts and the placement of the FSCL are at the heart of the matter" (David E. Johnson, *Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post–Cold War Era*, pp.130–31).

Olsen's edited volume impresses by the sheer number of prominent and distinguished authors that made the final product possible. The volume's unique angle on airpower combined with the input from some of the best airpower scholars adds to our understanding of the air service.

Dr. Christian F. Anrig
Deputy Director of Doctrine Research and Education
Swiss Air Force

Obama at War: Congress and the Imperial Presidency by Ryan C. Hendrickson. The University Press of Kentucky, 2015, 192 pp., $35.00.

The Constitution of the United States unequivocally bestows, and the War Powers Resolution (WPR) of 1973 further reinforces, the power to declare war to the Congress. In this book, Dr. Ryan C. Hendrickson points out every president (Democratic and Republican) since World War II has increasingly used the mantle of commander

in chief to apply military force in various situations without prior Congressional authorization. To show Pres. Barack Obama does not discriminate in the types of situations where he unilaterally acts, the author describes four examples: operations in Afghanistan, including the particular use of drone technology; combat against Indian Ocean piracy; military strikes against Libya; and the use of US fighting and consultation forces in South Sudan. In all of these cases, Congress has not directly authorized the use of military force application outside of the United States. It has either not taken up the issue for debate or key leaders of both parties have defended President Obama's actions.

It is this independent presidential deed and Congress's apparent willingness to allow the president to act in this manner that frames Hendrickson's thesis: Anytime any president individually authorizes the use of combat operations on foreign soil without the advice and consent of the joint Congress, he is acting unconstitutionally. Further, any Congress that does not use the inherent checks and balances mechanism to force the president to get the advice and consent of the joint Congress before committing those forces overseas is also acting unconstitutionally.

The author asserts that over the years since World War II, and through much iteration of presidential administrations and congresses, the authority to wage war has politically shifted from the legislative branch to the executive. The political majority in Congress has switched several times, but the outcome has remained the same, resulting in an evident congressional apathy and wide deference to the president to protect the United States. The author keys on the presumption that members of Congress are usually always in campaign and fundraising mode and must be very careful in how they are perceived by their constituents. Many are not likely to present a legitimate challenge; however, the author does describe a few "rebels" who make a bit of noise from time to time. Hendrickson details several efforts fronted by newer members of Congress attempting to reel in the presidential military power only to be thwarted by their own Congressional leaders. These establishment leaders are shown to go so far as to actively promote the president's flexible authority to conduct offensive military operations with prior congressional notification and consent. Their rationale echoes the president's argument that these actions are necessary for the commander in chief to protect the United States from harm.

To resolve this issue, the author looks to each of the federal government branches for recourse. When judicial cases have come forward from members of the House or Senate, federal courts have refused to hear the cases on the merits, citing the congressional plaintiff's lack of a justiciable legal question suitable for judicial review. The legislature does not have the right kind of leadership with the political willpower and equity to push for this kind of significant reform. The executive does not appear willing to retreat from the established position. Hendrickson asserts the only sure path back to the Constitution's foundations is for Congress to affirmatively wrest control from the presidency.

It is important for the reader to understand the very narrow scope of this book. The thesis does not go very far beyond the assertions that the president consistently acts in an unconstitutional manner and the Congress consistently acts in a somewhat

negligent manner. Alone and based on the facts, Hendrickson believes he is right and has a valid constitutional argument. To the extent he identifies the issue and discusses some clear ways to resolve it, he does so rather well—with ample research and documentation.

However, politics and national governance do not occur in a vacuum. One does not simply take a single piece of the big picture, examine it, point out its flaws, and consider the analysis complete. The entire context of the situation must be considered. Hendrickson fails to address the necessary and next logical steps. How would the outcome of these combat operations been different if Congress had explicitly authorized warfare? What negative implications, if any, would have been averted had Congress acted before the president? The author does not address these questions—even to say the outcome can never be truly known. He does not explain how the United States' national security posture would be different if Congress granted presidential war powers before each foreign conflict. Certainly if he could, the results might strengthen his position.

This book is a quick and enjoyable read that challenges the reader to think about the oft-debated argument of textual versus practical readings of the US Constitution. Words mean things, and reasonable minds can come to different conclusions based upon different interpretations of the same words. Hendrickson has a point: from a literal reading of the Constitution, many presidents and congresses since the second half of the last century have acted unconstitutionally. However, the realities of the modern world force the reader to decide if the president's authority as commander in chief allows the use of proactive military force in foreign lands and ultimately if the ends justify the means.

Maj Randall Mercer, USAF

Mission Statement

Strategic Studies Quarterly (*SSQ*) is the strategic journal of the United States Air Force, fostering intellectual enrichment for national and international security professionals. *SSQ* provides a forum for critically examining, informing, and debating national and international security matters. Contributions to *SSQ* will explore strategic issues of current and continuing interest to the US Air Force, the larger defense community, and our international partners.

Disclaimer

The views and opinions expressed or implied in *SSQ* are those of the authors and should not be construed as carrying the official sanction of the US Air Force, the Department of Defense, Air Education and Training Command, Air University, or other agencies or departments of the US government.

Comments

We encourage you to e-mail your comments, suggestions, or address change to: **StrategicStudiesQuarterly@us.af.mil**.

Article Submission

The *SSQ* considers scholarly articles between 5,000 and 15,000 words from US and international authors. Please send your submission in Microsoft Word format via e-mail to:

StrategicStudiesQuarterly@us.af.mil

— — — — — — — — — — — — — — — — — —

Strategic Studies Quarterly (SSQ)
155 N. Twining Street, Building 693
Maxwell AFB, AL 36112–6026
Tel (334) 953–7311
Fax (334) 953–1451

View *Strategic Studies Quarterly* online at **http://www.au.af.mil/au/ssq/**

Free Electronic Subscription

A forum for critically examining, informing, and debating national and international security.

"Aim High . . . Fly-Fight-Win"

SSQ Strategic Studies Quarterly WINTER 2015

AFRL AUMPRESS